

**CONTRATTO PER L'ACCESSO ALLA MENSA DELL'AZIENDA**

**OSPEDALIERO-UNIVERSITARIA CAREGGI DEI DIPENDENTI**

**DELL'AZIENDA USL TOSCANA CENTRO**

TRA

**L'AZIENDA OSPEDALIERO-UNIVERSITARIA CAREGGI DI**

**FIRENZE**, (di seguito denominata "Azienda") nella

persona del Direttore Generale Dott. Rocco Donato

Damone, nato a Tolve il 29.02.1956, domiciliato per

la carica presso la sede dell'Azienda Ospedaliera

stessa in Firenze, Largo Brambilla, 3- P. IVA

04612750481;

E

**L'AZIENDA USL TOSCANA CENTRO** (di seguito denominata

"AUSLTC") con sede in Firenze - Piazza S. Maria

Nuova, 1 (C.F. e P. IVA 04612810483), nella persona

del Direttore Generale dr. Paolo Morello Marchese

nato a Padova il 2.06.1956, domiciliato per la

carica nella sede stessa dell'Azienda;

**SI CONVIENE E SI STIPULA QUANTO SEGUE:**

**ART.1 - OGGETTO DELLA CONVENZIONE**

L'Azienda consentirà l'accesso alla propria mensa

ai dipendenti dell'AUSLTC i cui nominativi dovranno

essere preventivamente comunicati alla mail

[convenzioniecontratti@ao-u-careggi.toscana.it](mailto:convenzioniecontratti@ao-u-careggi.toscana.it) della

U.O.c Gestione Attività Libero Professionale e Area

pagamento dell'AOU Careggi , che provvederà alla trasmissione del medesimo alla propria U.O.c Gestione del Personale per i conseguenti adempimenti.

#### **ART. 2 - MODALITA' DI ESPLETAMENTO DEL SERVIZIO**

L'accesso alla mensa sarà consentito esclusivamente ai dipendenti dell' AUSLTC, indicati nella predetta comunicazione, ai quali l'Azienda fornirà badge aziendale nominativo per rilevarne la presenza.

#### **ART. 3 - COMPENSI PER L'ATTIVITA' SVOLTA**

L'AUSLTC per ogni pasto consumato da ciascun dipendente, sia nei giorni feriali che festivi, corrisponderà all'Azienda la somma di € 5,60 + IVA.

L'Azienda, emetterà mensilmente una fattura riepilogativa corredata da riepilogo nominativo con indicazione dei giorni e dell'ora di accesso alla propria mensa.

L'AUSLTC liquiderà e pagherà le fatture nel termine di 60 giorni dal ricevimento delle stesse attraverso il Sistema di Interscambio. Per quanto sopra si specificano i seguenti estremi identificativi:  
Codice Univoco Ufficio: **UFL7WY;**

I suddetti costi potranno essere variati, in corso di convenzione, dall'Azienda e comunicati tramite

PEC all'AUSLTC , che potrà accettare, ovvero rescindere la presente convenzione.

#### **ART. 4 - MODALITA' DI PAGAMENTO**

Il corrispettivo dovrà essere versato all'Azienda Ospedaliero-Universitaria Careggi con le seguenti modalità: girofondo sul conto Banca d'Italia - contabilità speciale 0306163 intestato a Azienda Ospedaliero-Universitaria Careggi.

#### **ART. 5 - TRATTAMENTO DEI DATI PERSONALI**

Il trattamento dei dati personali, di cui l'Azienda ed il suo personale vengano a conoscenza durante l'espletamento delle attività oggetto del presente atto, deve avvenire nel rispetto del Regolamento Europeo 2016/679 e (RGPD), del D.Lgs. 196/2003 e s.m.i. I dati forniti dalle Parti e relativi ai soggetti che per loro conto svolgono attività amministrative funzionali alla stipula e alla gestione del rapporto convenzionale, saranno trattati nel rispetto dei principi di liceità, correttezza, trasparenza, adeguatezza, pertinenza e necessità di cui all'art. 5, paragrafo 1 del RGPD. Il conferimento di tali dati tra le parti è comunque obbligatorio al fine di adempiere a tutti gli obblighi comunque connessi alla gestione ed esecuzione del rapporto instaurato con il presente

atto. Le parti si danno reciprocamente atto che le persone che agiscono per loro conto sono state informate sull'utilizzo dei propri dati personali.

Per quanto riguarda le attività previste nella presente convenzione, Titolare del trattamento è l'AUSL Toscana Centro e l'Azienda è nominata responsabile del trattamento dei dati.

Durata del trattamento, natura e finalità del trattamento, tipo di dati personali e categorie di interessati, obblighi e diritti del Titolare del trattamento sono disciplinati dall'atto redatto e sottoscritto, prima dell'inizio delle attività, ex art. 28 paragrafo 3 del Regolamento UE 679/2016.

#### **ART. 6 - DECORRENZA E DURATA**

La presente convenzione decorrerà dalla data della sottoscrizione e avrà durata triennale, salvo disdetta, riconosciuta ad entrambe le parti, da comunicarsi, mediante lettera raccomandata a/r. o PEC, con preavviso di 90 giorni.

Resta inteso che la disciplina della collaborazione contenuta nel presente accordo si applica anche alle obbligazioni conseguenti alle attività poste eventualmente in essere precedentemente, nelle more della contrattazione e formalizzazione del presente rapporto convenzionale.

#### **ART. 7 - NORME FINALI**

Per tutto quanto non espressamente previsto dal contratto si fa rinvio alle vigenti disposizioni in materia.

L'entrata in vigore di disposizioni normative di legge, successive al presente contratto, che rechino una disciplina diversa da quella in esso prevista, comporta l'immediata caducazione delle disposizioni incompatibili e la diretta applicazione della disciplina sopravvenuta fino al relativo adeguamento.

#### **ART. 8 - SPESE DI BOLLO, REGISTRAZIONE E FORO COMPETENTE**

La presente convenzione sarà registrata solo in caso d'uso a spese della parte che avrà interesse a farlo. Le spese di bollo della presente convenzione, sono a carico dell'AUSLTC che provvederà all'assolvimento virtuale.

Foro competente in via esclusiva per le controversie derivanti dall'applicazione del presente accordo è quello di Firenze.

#### **ART. 9 - FIRMA**

In base all'articolo 15, comma 2 bis della Legge 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso

*ai documenti amministrativi", il presente contratto è sottoscritto dalle parti con firma digitale, ai sensi dell'articolo 24 del decreto legislativo 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale".*

Il contratto consta di n.9 articoli, n. 6 pagine ed è conservato agli atti dalla competente Unità Operativa dell'Azienda

Azienda Ospedaliero-Universitaria Careggi

Il Direttore Generale

Dr. Rocco Donato Damone

Azienda USL Toscana Centro

Il Direttore Generale

Paolo Morello Marchese

**“ATTO GIURIDICO” DI DEFINIZIONE DELLE RESPONSABILITA’ IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**, ai sensi dell’art. 28 paragrafo 3 del Regolamento UE n° 679 del 27 aprile 2016 del Parlamento Europeo e del Consiglio (RGPD), a valere anche quale “istruzione documentata” di cui al medesimo articolo.

TRA

L'**Azienda USL Toscana Centro** con sede legale in Firenze, P.zza S.Maria Nuova, 1 50122 (FI), Partita IVA/codice fiscale 06593810481 (di seguito anche Azienda USL T.C. o Titolare) in persona del Direttore Generale Dr. Paolo Morello Marchese, domiciliato per la carica presso l'Azienda USL Toscana Centro stessa

E

L'Azienda Ospedaliero-Universitaria Careggi, con sede legale in Firenze - Largo Brambilla 3, P.I. 04612750481 (di seguito anche “AOU Careggi” o “Responsabile”), in persona del Direttore Generale Dr. Rocco Donato Damone, domiciliato per la carica presso l'Azienda Ospedaliero-Universitaria stessa

Congiuntamente indicate come le “Parti”

Visti:

- il *Regolamento generale 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* ... (di seguito: RGPD);
- il *D.Lgs. 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679* ... (di seguito: Codice).

Premesso che:

- ai sensi delle normative vigenti, il Titolare è il soggetto che:
  - o tratta dati personali nel proprio interesse (o per scopi di interesse pubblico che sono ricompresi tra i suoi fini istituzionali) determinando (o perlomeno facendo proprie) le finalità del trattamento e predisponendone(o condividendone) le modalità;
  - o tratta tali dati in maniera esclusiva, e può perciò decidere autonomamente se altri soggetti possano collaborare, nell'interesse del Titolare stesso, al trattamento, e come e quando questi devono acquisire quei dati e successivamente perderne la disponibilità (cancellandoli o restituendoli);
  - o fornisce istruzioni sulle modalità del trattamento ai soggetti, persone fisiche o meno, che lo effettuano sotto la sua autorità o nel suo interesse;
  - o detiene i dati e può successivamente utilizzarli o cederli per proprie ulteriori finalità, ivi comprese quelle di cui all'art. 99 del Codice.
- ai sensi delle normative vigenti il Responsabile è il soggetto che svolge attività di trattamento “per conto del Titolare”, ovvero nell'ambito di una delega di funzioni, e dunque:
  - o sulla base di una decisione del Titolare, formalizzata in un contratto o altro atto giuridico, che fornisce al Responsabile la legittimazione in concreto (cioè nel caso specifico) ad effettuarla, della quale altrimenti sarebbe privo;
  - o sulla base di istruzioni del Titolare, mantenendo al di fuori di queste i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle attività delegate, e le connesse responsabilità;
  - o detenendo i dati temporaneamente, per il tempo concordato con il Titolare, e non potendo ulteriormente utilizzarli o cederli per finalità proprie o per le ulteriori finalità di cui all'art. 99 del Codice.

- alcune funzioni proprie o di interesse di Azienda USL T.C. devono essere esternalizzate alla AOU Careggi, nell'ambito del contratto per l'accesso alla mensa dell'AOU Careggi dei dipendenti dell'Azienda USL T.C.;
- tale esternalizzazione di funzioni comporta che, per poter svolgere le conseguenti attività, la AOU Careggi, debba trattare dati personali per conto della Azienda USL T.C.;
- Azienda USL T.C., relativamente alle attività di trattamento di cui al punto precedente, si qualifica quale Titolare del trattamento ai sensi dell'art. 4 paragrafo 7 del RGPD;
- la AOU Careggi, relativamente alle suddette attività di trattamento, svolge il ruolo di Responsabile del trattamento ai sensi dell'art. 4 paragrafo 8 e dell'art. 28 del RGPD;
- l'art. 28 del RGPD prescrive che i trattamenti svolti da parte del Responsabile del trattamento per conto del Titolare siano disciplinati da un contratto o altro atto giuridico vincolante per il Responsabile, che individui la materia del trattamento, la durata, la natura e la finalità, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
- la AOU Careggi dichiara di essere in possesso dei necessari requisiti di conoscenza specialistica, affidabilità e risorse tali da fornire sufficienti garanzie per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa vigente e garantisca la tutela dei diritti dell'interessato;
- con la sottoscrizione del presente documento secondo quanto disposto dall'art. 28 del RGPD, le Parti intendono regolare i reciproci rapporti in relazione al trattamento dei dati personali effettuato dalla AOU Careggi per conto di Azienda USL T.C.;

tutto ciò premesso, le Parti convengono e stipulano quanto segue:

#### ART. 1

(Oggetto, finalità e durata del trattamento)

Il trattamento può essere brevemente descritto come segue:

ogni trattamento di dati personali che sia funzionale e necessario ad adempiere agli obblighi comunque connessi alla gestione ed esecuzione del rapporto instaurato con il contratto per l'accesso alla mensa dell'AOU Careggi dei dipendenti dell'Azienda USL T.C..

Le basi giuridiche del trattamento sono individuabili dei seguenti articoli del RGPD/Codice:

- Art. 6, par.1, lettera c) del RGPD: "Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento";
- Art. 9, par.2, lettera b) del RGPD: "Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia del diritto del lavoro (..)";
- Art.2-sexies, comma 2, lettera dd) del Codice.: "instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo (..)";

Il trattamento riguarda le seguenti tipologie di interessati:

- dipendenti dell'Azienda USL T.C.

Il trattamento ricomprende le seguenti tipologie di dati:

- dati personali (art. 4 n. 1 del RGPD) rientranti nelle categorie "particolari" di dati personali (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale, all'orientamento sessuale della persona) di cui all'art. 9 del RGPD;
- dati personali di cui all'art. 4 n. 1 del RGPD che non rientrano né tra le categorie particolari di dati di cui all'art. 9 del RGPD né in quelli relativi alle condanne penali e ai reati o a connesse misure di sicurezza di cui all'art. 10 RGPD (dati cd. "comuni" come ad es: dati anagrafici quali nome e cognome, anno di nascita, sesso; dati di contatto, indirizzo email, recapito di telefonia fissa o mobile).

I dati sono trattati con modalità:



- identificativa;
- codificata
- pseudonimizzata;

Il trattamento è effettuato con strumenti:

- informatici
- cartacei

Con la sottoscrizione del presente atto Azienda USL T.C. individua la AOU Careggi quale Responsabile del trattamento di cui sopra, con l'incarico di effettuare le operazioni di trattamento sui dati personali di cui entra in possesso od a cui ha comunque accesso, nell'esecuzione delle attività specificate in premessa.

La AOU Careggi, con la sottoscrizione del presente atto, conferma la diretta e approfondita conoscenza degli obblighi che assume in relazione alla disposizioni normative e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina.

La AOU Careggi prende atto che l'incarico di effettuare le operazioni di trattamento dei dati personali quale Responsabile del trattamento è affidato in quanto il suo profilo è stato ritenuto idoneo a soddisfare i requisiti di conoscenza specialistica, affidabilità e risorse tali da fornire sufficienti garanzie per mettere in atto misure tecniche ed organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti della normativa vigente e garantisca la tutela dei diritti dell'interessato. Qualsiasi mutamento di tali requisiti che possa determinare incertezze sul mantenimento dei requisiti stessi, deve essere comunicato al Titolare che può esercitare in piena autonomia e libertà di valutazione il diritto di recesso, senza penali o oneri a proprio carico.

Il presente atto di nomina ha validità per il tempo necessario ad eseguire le attività affidate al responsabile, e si considera venuto meno al termine delle attività stesse o qualora venga meno il rapporto con il Titolare.

## ART. 2

### (Obblighi del Responsabile e modalità di trattamento)

Il Responsabile del trattamento, relativamente ai dati personali oggetto di trattamento, ha l'obbligo di attenersi alle istruzioni di seguito riportate e a quelle ulteriori impartite dal Titolare mediante procedure e/o comunicazioni specifiche.

Il Responsabile del trattamento, relativamente ai dati personali oggetto di trattamento, è tenuto a:

- organizzare, gestire e supervisionare tutte le operazioni di trattamento di competenza attenendosi ai principi generali e alle disposizioni della vigente normativa in materia di protezione dei dati personali, ovvero, assicurare che i dati personali oggetto del trattamento siano:
  - ✓ trattati in modo lecito e secondo correttezza;
  - ✓ raccolti e registrati per scopi determinati, espliciti e legittimi; a tale riguardo, l'utilizzazione di dati personali e di dati identificativi dovrà essere ridotta al minimo, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi, ovvero adottando modalità che permettano di identificare gli interessati solo in caso di necessità;
  - ✓ esatti e, se necessario, aggiornati;
  - ✓ pertinenti, completi e non eccedenti rispetto alle finalità del trattamento;
- effettuare il trattamento dei dati con logiche e modalità strettamente ed esclusivamente correlate alle finalità di cui all'art. 1, per il tempo strettamente necessario per il perseguimento delle finalità connesse, garantendo il pieno rispetto delle istruzioni ricevute;
- informare immediatamente l'Azienda qualora, a suo parere, l'applicazione di una sua istruzione possa violare, nel concreto contesto operativo, le disposizioni in materia di protezione dei dati personali;

- tenere il Registro delle attività di trattamento, ex art. 30 par. 2 del RGPD;
- conservare e custodire con diligenza, prudenza e perizia i dati personali oggetto del trattamento;
- sono fatti salvi eventuali obblighi di conservazione previsti dalla normativa, obblighi che il Responsabile è tenuto a motivare impegnandosi a non compiere sui dati conservati, e a non consentire ai propri sub-Responsabili, operazioni di trattamento per qualsivoglia ulteriore finalità,
- restituire all'azienda, in caso di cessazione dell'accordo in essere tra le Parti, qualsiasi dato personale, su qualsiasi supporto, di cui sia entrato in possesso, senza che alcun dato possa essere direttamente o indirettamente detenuto;
- mantenere riservati, non comunicare e diffondere a terzi i dati personali e le informazioni di cui è venuto a conoscenza per effetto del trattamento;
- non utilizzare i dati personali e le informazioni, anche se in forma anonimizzata o pseudonimizzata, comprese le eventuali elaborazioni realizzate su disposizione di Azienda USL T.C.;
- assistere il Titolare nel garantire il rispetto degli obblighi relativi alla sicurezza del trattamento, alla notifica di una violazione dei dati personali all'Autorità di controllo (vedi art. 9), alla comunicazione di una violazione di dati personali all'interessato (vedi art. 9), alla valutazione d'impatto sulla protezione dei dati personali (vedi art. 11), alla consultazione preventiva dell'Autorità di controllo ove normativamente previsto;
- attenersi alle specifiche disposizioni previste per il trasferimento di dati all'estero, qualora necessario (vedi art. 4), ed a non effettuare in alcun caso operazioni di diffusione dei dati stessi;
- mettere a disposizione del Titolare del trattamento tutte le informazioni e i documenti necessari a dimostrare il rispetto degli obblighi previsti dalla vigente normativa per il Responsabile del trattamento dati;
- assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato previsti dagli artt. 15-19 e 21 del RGPD; qualora il Responsabile riceva richieste da parte di interessati finalizzate all'esercizio dei propri diritti, esso dovrà:
  - ✓ darne tempestiva comunicazione al Titolare con comunicazione di posta elettronica certificata allegando copia delle richieste;
  - ✓ coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni aziendali designate dal Titolare per gestire le relazioni con gli interessati;
  - ✓ assistere e supportare il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste di esercizio dei diritti degli interessati, negli ambiti e nel contesto del ruolo in cui opera il Responsabile del trattamento.

### ART. 3

#### (Soggetti autorizzati al trattamento dei dati)

Il Responsabile del trattamento si impegna:

- a individuare formalmente quali soggetti autorizzati al trattamento coloro che, a qualunque titolo, devono compiere per suo conto operazioni del trattamento e/o attuare compiti relativi alla protezione e alla libera circolazione dei dati limitando l'accesso e il trattamento ai soli dati necessari per lo svolgimento delle attività consentite rispetto alle mansioni svolte;
- a impartire per iscritto ai soggetti autorizzati, appropriate e complete istruzioni su come svolgere correttamente ed in modo lecito il trattamento,
- a vigilare regolarmente sulla puntuale osservanza delle istruzioni impartite da parte dei soggetti autorizzati, anche mediante verifiche periodiche;
- a curare la formazione specifica in materia di protezione dei dati personali dei soggetti autorizzati che operano sotto la sua responsabilità;

- a garantire che i propri dipendenti e/o collaboratori che operano a vario titolo nell'ambito del rapporto in essere con l' Azienda, siano dotati di esperienza, capacità e affidabilità con riferimento alla gestione dei sistemi informatici in particolare per quanto attiene alle misure di sicurezza previste dalla normativa in materia di protezione dei dati..

#### ART.4 (Responsabile della Protezione dei Dati)

Il Responsabile– ove tale obbligo si applichi anche al Responsabile stesso in base alle disposizioni dell'art. 37 del RGPD – si impegna a nominare e comunicare al Titolare il nominativo e i dati di contatto del Responsabile della Protezione dei Dati.

#### ART.5 (Trasferimento verso paesi terzi o organizzazioni internazionali)

Il Responsabile si impegna a circoscrivere gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione, conservazione dei dati sui propri server) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in Paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione europea, clausole contrattuali modello, consenso degli interessati, ecc.).

Il Responsabile pertanto non dovrà trasferire o effettuare il trattamento dei dati personali del Titolare del trattamento al di fuori dell'Unione Europea per nessuna ragione, in assenza di autorizzazione scritta da parte del Titolare.

Qualora, in corso di esecuzione del Contratto, il Titolare rilasci tale autorizzazione e venga pertanto effettuato un trasferimento di dati personali del Titolare del trattamento al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare le previsioni di cui al Regolamento UE 2016/679.

Resta inteso fra le Parti che il Responsabile dovrà garantire che i metodi di trasferimento impiegati, anche in conformità alle clausole contrattuali standard approvate dalla Commissione Europea ed ai presupposti indicati nella medesima decisione, consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata del presente atto di nomina.

Il Responsabile è obbligato a comunicare immediatamente al Titolare il verificarsi delle seguenti fattispecie:

- mancato rispetto delle clausole contrattuali standard di cui sopra;
- qualsiasi modifica dei metodi e delle finalità di trasferimento dei dati personali del Titolare all'estero.

#### ART.6 (Misure di sicurezza)

Con riguardo alle misure di sicurezza da osservare nel trattamento dei dati e allo scopo di ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità ivi previste, il Responsabile del trattamento si impegna:

- ad adottare adeguate ed idonee misure tecniche ed organizzative previste dalla normativa italiana ed europea in materia di protezione dei dati personali ed ogni altra previsione derivante dall'Autorità di controllo e dal Comitato Europeo per la protezione dei dati, curandone il rispetto e l'applicazione da parte degli autorizzati al trattamento, effettuando, altresì controlli sull'operato dei medesimi;
- a verificare periodicamente e, ove necessario, ad adeguare le misure di sicurezza con riferimento all'analisi dei rischi aziendali, all'evolversi della normativa e al progredire dello sviluppo tecnologico;

- a garantire le evidenze e la documentazione comprovanti l'adozione delle misure tecniche ed organizzative idonee.

#### ART.7 (Controlli)

Il Responsabile si impegna a consentire al Titolare la verifica del rispetto del presente atto di nomina .

Il Responsabile si impegna a supervisionare e controllare direttamente i soggetti da esso designati per le operazioni di trattamento.

Il Responsabile riconosce al Titolare il diritto di effettuare controlli relativamente alle operazioni aventi ad oggetto il Trattamento dei dati personali ed a tal fine il Titolare, ove lo reputi opportuno, potrà disporre verifiche a campione o attività di audit avvalendosi di personale espressamente incaricato a tale scopo.

Il Responsabile si impegna a mettere a disposizione in qualunque momento e dietro richiesta del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina e a contribuire alle attività di controllo, comprese eventuali ispezioni realizzate dal Titolare del Trattamento o altro soggetto incaricato. Tutti i controlli potranno essere effettuati periodicamente in base a metodologie concordate tra le Parti.

#### ART.8 (Nomina dei sub Responsabili del trattamento)

Il Responsabile del trattamento è autorizzato a ricorrere, ai sensi di quanto previsto dall'art. 28 par. 4 del RGPD, ad altro soggetto (di seguito sub Responsabile del trattamento) per l'esecuzione di specifiche attività di trattamento per conto del Titolare, disciplinando il rapporto con atto giuridico o contratto teso a circoscrivere i rispettivi ambiti di responsabilità e facendo sottoscrivere al sub Responsabile le medesime condizioni applicate nel presente atto di nomina adottando nei confronti dello stesso gli stessi obblighi in materia di protezione di dati personali già in capo al Responsabile del trattamento e derivanti dalla sottoscrizione del presente atto di nomina.

Il Responsabile del trattamento dovrà assicurare che il sub Responsabile del trattamento offra garanzie sufficienti di affidabilità e riservatezza e metta in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD e che restituisca *[ovvero cancelli]* i dati personali oggetto dei trattamenti e le eventuali copie al termine della prestazione del servizio.

Il sub Responsabile del trattamento potrà trattare i dati personali nella misura in cui il trattamento sia strettamente necessario per l'esecuzione del Contratto in essere tra le Parti ed in ogni caso nel rispetto del presente atto di nomina, restando inteso tra le Parti che il sub Responsabile sarà inoltre obbligato al rispetto delle limitazioni cui il Fornitore è tenuto.

Qualora l'eventuale sub Responsabile, esecutore del trattamento, ometta di adempiere ai propri obblighi in materia di protezione dei dati personali, il Responsabile dichiara espressamente e garantisce di mantenere l'intera responsabilità dell'adempimento degli obblighi di tale soggetto.

Il Responsabile del trattamento dovrà trasmettere all'Azienda la denominazione del sub Responsabile del trattamento, nonché di ogni altra modifica riguardante l'aggiunta o la sostituzione con altri sub Responsabili del trattamento, dando al Titolare la possibilità di opporsi.

#### ART.9 (Responsabilità)

Il Responsabile del trattamento risponde per il danno causato dal trattamento se non ha adempiuto agli obblighi del RGPD specificatamente diretti al responsabile del trattamento, o ha agito in modo difforme o contrario rispetto alle istruzioni offerte dal Titolare.

Il Responsabile del trattamento si obbliga a tenere manlevata ed indenne il Titolare da ogni responsabilità o danno, anche nei confronti di terzi, e da qualunque somma che il Responsabile del trattamento dovesse essere condannato a pagare, derivante direttamente o indirettamente da fatti attivi o omissivi ad esso imputabili esclusivamente, commessi anche dai dipendenti e/o

collaboratori che operano a vario titolo come autorizzati al trattamento dei dati, ivi inclusi i danni derivanti dalla perdita, sottrazione, deterioramento e/o distruzione dei dati trattati.

Il Responsabile del trattamento conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del sub Responsabile del trattamento, qualora quest'ultimo ometta di adempiere agli obblighi in materia di protezione dei dati disciplinati nel RGPD o nel presente atto.

#### ART. 10

(Violazione dei dati personali c.d. *data breach*)

In eventuali casi di violazione dei dati personali consistenti nella violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare del trattamento, il Responsabile deve:

- informare il Titolare, con comunicazione da inviarsi all'indirizzo PEC dello stesso, , tempestivamente e in ogni caso non oltre le 24 ore dalla scoperta dell'evento, di essere venuto a conoscenza di una violazione allegando alla comunicazione la scheda evento (allegato 1. al presente atto) ) recante le seguenti dettagliate informazioni:
  - ✓ la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  - ✓ il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso il Responsabile da cui ottenere maggiori informazioni;
  - ✓ le probabili conseguenze della violazione dei dati personali;
  - ✓ le misure adottate per mitigare i rischi;
- fornire ove possibile assistenza al Titolare del trattamento per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti;
- attivarsi per mitigare, ove possibile, gli effetti delle violazioni proponendo tempestive azioni correttive al Titolare ed attuando tempestivamente tutte le azioni correttive approvate e/o richieste dal Titolare stesso.

#### ART. 11

(Valutazione di impatto sulla protezione dei dati)

Con riferimento agli artt. 35 e 36 del RGPD, il Responsabile si impegna, su richiesta, ad assistere il Titolare nelle attività necessarie all'assolvimento degli obblighi previsti dai succitati articoli, sulle base delle informazioni in proprio possesso, in ragione dei trattamenti svolti in qualità di Responsabile del trattamento, ivi incluse le informazioni relative agli eventuali trattamenti effettuati dai sub - Responsabili.

#### ART. 12

(Amministratori di sistema)

Il Responsabile, ove applicabile, assume le funzioni e le responsabilità dei cd. amministratori di sistema di cui al provvedimento dell'Autorità Garante per la protezione dei dati personali *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* del 27 novembre 2008 e successive modifiche ed integrazioni, e si impegna a svolgere tali attività nel rispetto delle prescrizioni ivi contenute.

#### Art.13.

(Restituzione e cancellazione dei dati)

In caso di cessazione del contratto/convenzione, Il Responsabile provvede , a scelta e su richiesta del Titolare, alla restituzione dei dati, comprese le eventuali copie di backup e tutta la documentazione cartacea, oppure alla integrale cancellazione/distruzione degli stessi, rilasciando in ogni caso attestazione scritta che presso di se non ne sussiste copia alcuna.

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

Sono fatti salvi eventuali obblighi di conservazione previsti dalla normativa, obblighi che il Responsabile è tenuto a motivare impegnandosi a non compiere sui dati conservati, e a non consentire ai propri sub-Responsabili, operazioni di trattamento per qualsivoglia ulteriore finalità.

#### ART. 14 (Accettazione della nomina)

Con la sottoscrizione del presente atto, ai sensi dell'art.28 del Regolamento UE 2016/679, il Responsabile accetta la propria nomina, in relazione ai dati personali la cui conoscenza risulta essere indispensabile per l'adempimento delle obbligazioni di cui al Contratto in essere tra le Parti. Il Responsabile è a conoscenza degli obblighi previsti dal Regolamento UE 2016/679 e del D.Lgs. n.196/2003 e successive modifiche e integrazioni e dovrà attenersi per lo svolgimento dei compiti assegnatigli alle previsioni e ai compiti contenuti nel presente atto di nomina. La presente nomina avrà durata fino alla cessazione, per qualsivoglia motivo, del Contratto in essere tra le Parti.

L'AZIENDA OSPEDALIERO- UNIVERSITARIA CAREGGI

L'AZIENDA USL TOSCANA CENTRO

**ALLEGATO 1 – SCHEDA EVENTO DATA BREACH**

| SCHEDA EVENTO                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Struttura interessata</b>                                                                                                                        |
| Data della violazione anche solo presunta (specificando se è presunta) <sup>i</sup>                                                                 |
| Data in cui si è avuto conoscenza della violazione                                                                                                  |
| Fonte della segnalazione                                                                                                                            |
| Tipologia violazione <sup>ii</sup>                                                                                                                  |
| Causa della violazione <sup>iii</sup>                                                                                                               |
| Descrizione violazione                                                                                                                              |
| Tipologia di dati oggetto della violazione <sup>iv</sup>                                                                                            |
| Dispositivo o supporto oggetto della violazione <sup>v</sup>                                                                                        |
| Sintetica descrizione dei sistemi di elaborazione o di memorizzazione o archiviazione dei dati coinvolti, con indicazione della relativa ubicazione |
| Numero interessati coinvolti <sup>vi</sup>                                                                                                          |
| Categorie di interessati coinvolti <sup>vii</sup>                                                                                                   |
| Luogo o ambito di trattamento in cui è avvenuta la violazione dei dati <sup>viii</sup>                                                              |
| Misure tecnologiche ed organizzative applicate ai dati oggetto di violazione <sup>ix</sup>                                                          |
| Azioni effettuate per contenere o minimizzare le conseguenze della violazione dei dati                                                              |

Data.....

Nome/cognome e ruolo ricoperto .....

Firma .....

Da inviare, secondo quanto indicato nell'articolo 2 della P/903/257, a: [rpd@aou-careggi.toscana.it](mailto:rpd@aou-careggi.toscana.it)

iii ... / Dal ... (violazione ancora in corso) / Dal ... al ... / In un tempo non ancora determinato.

ii Lettura (presumibilmente i dati non sono stati copiati) / copia (i dati sono ancora presenti sui sistemi del Titolare) / alterazione (i dati sono presenti sui sistemi ma sono stati alterati) / cancellazione (i dati non sono più sui sistemi del Titolare e non sono in possesso dell'autore della violazione) / Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione) / Altro (specificare)

iii Azione intenzionale interna / azione accidentale interna / azione intenzionale esterna / azione accidentale esterna / sconosciuta / altro (specificare)

iv Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...) / dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) / dati di accesso e di identificazione (username, password, customer id, altro...) / dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...) / dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...) / dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione / dati di profilazione / dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...) / dati di localizzazione / dati che rivelino l'origine razziale o etnica / dati che rivelino opinioni politiche / dati che rivelino convinzioni religiose o filosofiche / dati che rivelino l'appartenenza sindacale / dati relativi alla vita sessuale o all'orientamento sessuale / dati relativi alla salute / dati genetici / dati biometrici / altro (specificare).

v Banca dati elettronica / personal computer / dispositivo di acquisizione o dispositivo-lettore / smart card o analogo supporto portatile / file o parte di un file / strumento di back up / rete / documento cartaceo / altro (specificare).

vi Indicare il numero preciso oppure quello stimato oppure che il numero è ancora sconosciuto.

vii Dipendenti / collaboratori / Contraenti / Pazienti / Minori / Altro (specificare).

viii Specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili.

ix Pseudonimizzazione e cifratura dati personali / assicurazione su base permanente della riservatezza, dell'integrità, della disponibilità e della resilienza dei sistemi e dei servizi di trattamento / ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico / verifica e valutazione sistematica dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento / limitazione della quantità di dati acquisiti (principio di minimizzazione) / chiavi robuste di autenticazione / idonei controlli sugli accessi / back up sicuri