REGOLAMENTO AZIENDALE SULLA PROTEZIONE DEI DATI PERSONALI Versione 2

AZIENDA OSPEDALIERA PUGLIESE CIACCIO DI CATANZARO

Relativo alla Protezione delle Persone Fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati

SOMMARIO

Parte I
Disposizioni generali

ARTICOLO 1 -Oggetto

Il presente regolamento dell'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro contiene disposizioni organizzative ed attuative del Regolamento UE 2016/679, delle linee guida emanate dal Comitato Europeo per la protezione dei dati, dal vigente D. Lgs. n. 196/03 così come novellato dal D. Lgs. 101/18 e da tutte le pronunce dell'Autorità Garante per la Privacy, nell'ambito delle strutture, servizi e presidi della medesima azienda, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli utenti e di tutti coloro che hanno rapporti con la stessa.

Secondo il considerando numero 1 del Regolamento UE 2016/679:

"La protezione delle persone fisiche con riguardo al trattamento del *dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e 1'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano."*

Secondo il considerando numero 2 del Regolamento UE 2016/679:

"I principi e le norme ci tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di liberò, Sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato inferno e al benessere delle persone fisiche."

L'articolo numero 1 del Regolamento UE 2016/679

"... stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati." Il suddetto regolamento inoltre. *protegge* i *diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei eletti personali La libera circolo ione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."*

L' dell'Azienda Ospedaliera "Pugliese Ciaccio" assicura l'adozione di misure di sicurezza anche preventive idonee ad evitare situazioni di rischio e non conformità o di alterazione di dati.

L' dell'Azienda Ospedaliera "Pugliese Ciaccio" adotta, altresì, le misure occorrenti per facilitare 1'esercizio dei diritti dell'interessato ai sensi degli articoli 12-23, contenuti nel Capo III del Regolamento UE 2016/679.

ARTICOLO 2 — Definizioni
Dato Personale - dati genetici - dati biometrici — dati relative alla salute — categorie particolari di dati personali

Per dato personale ai sensi dell'articolo 4 paragrafo 1 numero 1) del Regolamento Ue 2016/679 si intende: *qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato "),' si considera identificabile lo persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o* più *elementi caratteristici della sua* identità *fisica, fisiologica, genetica, psichica, economica, culturale o sociale,' (C26, C27,C30)*

Per **dati genetici** ai sensi dell'articolo 4 paragrafo 1 numero 13) Regolamento Ue 2016/679 si intendono: *i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione,' (C34)*

Per **dati biometrici** ai sensi dell'articolo 4 paragrafo 1 numero 14) Regolamento Ue 2016/679 si intendono: *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisici che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici,' (C51)*

Per **dati relative alla salute** ai sensi dell'articolo 4 paragrafo 1 numero 15) Regolamento Ue 2016/679 si intendono: *i dati personali* attinenti *alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano* informazioni *relative al suo stato di salute, (C35).*

Per **categorie particolari di dati personali** ai sensi dell'articolo 9 paragrafo 1 si intendono: *dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché dati genetici, dati* biometrici *intesi ci identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (C51)* Tale trattamento di dati personali è vietato.
Sono previste delle specifiche esenzioni al cennato divieto, infatti i suddetti dati sono trattati principalmente nell' dell'Azienda Ospedaliera "Pugliese Ciaccio" : in base al combinato disposto dell'articolo 9 paragrafo 2 lettera h) del Regolamento Ue 2016/679 con 1'articolo 9 paragrafo 3 del Regolamento Ue 2016/679 che così recitano: *lettera h) il trattamento è necessario per finalità li medicina preventiva o di medicina del lavoro, valutazione della capacità* lavorativa *del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto*

Dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità , fatte salve le condizioni e le garanzie di cui al paragrafo 3, (C53)

3. *I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la* responsabilità *di un professionista soggetto al segreto professionale conformemente al diritto dell'unione o degli* Stati *membri o alle norme* stabilite *dagli organismi nazionali competenti o da altra persona anch'essa soggetta*
all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme

stabilite dagli organismi nazionali competenti. (C53)
nonché in base all'articolo 9 paragrafo 2 lettera i) del Regolamento Ue 2016/679 che così recita:
lettera i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, gi f/f la *protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale,' (C54)*

ARTICOLO 3 — Trattamento dei dati personali

Con la definizione "trattamento", ai sensi dell'articolo 4, paragrafo 1, numero. 2) del Regolamento UE 2016/679 si intende: "qualsiasi *operazione o insieme di operazioni, compiute con o senza 1'ausilio di processi automatizzati* e *applicate e dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, 1'adattamento o la modifica, 1'estrazione, lei consultazione, 1'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra*

forma di *messa a disposizione,* il *raffronto o 1'interconnessione, la limitazione, la cancella ione o la distruzione";*
Il trattamento dei dati attiene alla responsabilità del Titolare del trattamento e dell'eventuale contitolare, ove previsto e presente e viene all'uopo delegato ai soggetti interni autorizzati al trattamento dei dati. Vi sono ipotesi in cui il trattamento dei dati viene, altresì, svolto in nome e per conto del titolare dai responsabili esterni al trattamento dei dati.

Parte II - I soggetti

Articolo 4 — Titolare del trattamento dei dati personali

Il principio cardine introdotto dal Regolamento UE 2016/679 è quello della responsabilizzazione" *(accountability)* che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della conformità" *o compliance),*

Il titolare ha l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare 1'applicazione del Regolamento UE 2016/679.

Il Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto verso l'esterno.

Per **titolare del trattamento,** ai sensi dell'articolo 4 paragrafo 1 numero 7 del Regolamento Ue 2016/679 si intende: *"la persona* fisica *o giuridica,*
/'autorità pubblica, *il servizio o altro organismo che, singolarmente o* ***insieme*** *ad altri, determina*

le finalità e i mezzi del trattamento di dati personali, quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o criteri specifici a*pplicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri",* (C74)

Nel caso di specie il titolare del trattamento è l'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro legalmente rappresentata dal Commissario Straordinario pro tempore.
Il Titolare nei casi previsti dal Regolamento UE 2016/679:

1. mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 2016/679, così come previsto dall'articolo 24 paragrafo 1 del Regolamento UE 2016/679;

2. le misure di cui al punto 1 sono riesaminate e aggiornate qualora necessario, così come previsto dall'articolo 24 paragrafo 1 del Regolamento UE 2016/679

3. determina e provvede all'attuazione di politiche adeguate in materia di protezione dei dati, così come previsto dall'articolo 24 paragrafo 2 del Regolamento UE 2016/679;

4. aderisce, ove possibile, ai codici di condotta di cui all'articolo 40 del Regolamento UE 2016/679 o a un meccanismo di certificazione di cui all'articolo 42 del Regolamento UE 2016/679, così come indicato dall'articolo 24 paragrafo 2 del Regolamento UE 2016/679:

5. mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione e la minimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, ed ad

6. integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti di protezione dei dati fin dalla progettazione del Regolamento UE 2016/679 e tutelare i diritti degli interessati, così come previsto dall'articolo 25 paragrafo 1 del Regolamento UE 2016/679; (c.d. privacy by design)

7. mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati e protetti, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza 1'intervento della persona fisica, così come previsto dall'articolo 25 paragrafo 2 del Regolamento UE 2016/679; (c.d. privacy by default).

8 nel caso in cui si individui un rapporto di contitolarità del trattamento dei dati, predispone, insieme all'altro contitolare in modo trasparente, un accordo interno, mediante il quale si determinano le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, così come previsto dall'articolo 26 del Regolamento UE 2016/679;

9 qualora un trattamento dei dati debba essere effettuato per suo conto da un soggetti esterno all'azienda, il titolare ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato, cosi come previsto dall'articolo 28 del Regolamento UE 2016/679;

10 i rapporti di cui al punto precedente tra il titolare del trattamento ed il responsabili esterno del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto del1'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che indichi la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, cosi come previsto dall'articolo 28 del Regolamento UE 2016/679;

11 *i soggetti interni individuati e designato come previsto dal punto precedente e che hanno accesso a dati personali non possono trattare tali dati se non istruiti dal titolare del trattamento stesso, cosi come previsto dall'articolo 29 del Regolamento UE 2016/679;*

12 i soggetti interni individuati e designato come previsto dal punto precedente e che hanno accesso a dati personali non possono trattare tali dati se non istruiti dal titolare del trattamento stesso, cosi come previsto dall'articolo 29 del Regolamento UE 2016/679;

13 tiene i Registri delle attività di trattamento svolte sotto la propria responsabilità. Tali registri contengono tutte le seguenti informazioni richieste ed indicate dall'articolo o0 del Regolamento UE 2016/679;

14) mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio così come previsto dall'articolo 2 del Regolamento UE 2016/679;

15) provvede alla notifica di una eventuale violazione dei dati personali all'autorità di controllo se ne ricorrono i presupposti, così come previsto dall'articolo 3e del Regolamento UE 2016/679;

16) provvede alla comunicazione di una eventuale violazione dei dati personali all'interessato se ne ricorrono i presupposti, così come previsto dall'articolo 34 del Regolamento UE 2016/679;

17) effettua, ove ne ricorrono i presupposti e prima di procedere al trattamento dei dati personali, la valutazione d'impatto sulla protezione dei dati, così come previsto dall'articolo 35 del Regolamento UE 2016/679;

18) allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, così come previsto dall'articolo 35 del Regolamento UE 2016/679;

19) qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo o5 indica che il trattamento presenta un rischio elevato in assenza di misure adottate dal titolare del trattamento, per attenuare il rischio prima di procedere al trattamento, consulta l'autorità di controllo, così come previsto dall'articolo 35 del Regolamento UE 2016/679;

20) designa sistematicamente un responsabile della protezione dei dati, così come previsto dall'articolo 37 del Regolamento UE 2016/679;

Articolo 5 — Responsabile della protezione dei dati (RPD) / Data Protection Officer (DPO)

Il titolare del trattamento designa sistematicamente un Responsabile della protezione dei dati (RPD) / Data Protection Officer (DPO), così come previsto dall'articolo 37 lettera a) del Regolamento UE 2016/679.
I compiti del Responsabile della protezione dei dati (RPD) / Data Protection Officer (DPO), così come previsto dall'articolo 39 del Regolamento UE 2016/679, sono i seguenti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

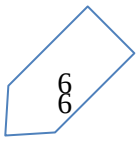
sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi 1'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

a) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo o5;

b) cooperare con 1'autorità di controllo; e

c) fungere da punto di contatto per 1'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro ha designato con deliberazione del Direttore Generale n. 225/ del 22 Maggio 2018 il Responsabile della protezione dei dati (RPD) / Data Protection Officer (DPO) ai sensi dell'art. 7 lettera a) del Regolamento Ue 2016/679, ha pubblicato i suoi dati di contatto sul sito aziendale ed ha comunicato la suddetta designazione all'autorità di controllo, così come previsto dall'articolo 37 paragrafo 7 del Regolamento Ue 2016/679.


6
6

Articolo 6 — Cooperazione con 1'autorità di controllo

L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro in qualità di titolare del trattamento coopera, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti, così come previsto dall'articolo 31 del Regolamento UE 2016/679.

Articolo 7 — Responsabili esterni del trattamento dei dati personali

L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro in qualità di titolare del trattamento dei dati individua gli Enti, gli organismi, altri soggetti pubblici o privati esterni all'Azienda nonché quelle strutture accreditate alle quali sono affidate attività o servizi, con esclusivo riferimento alle operazioni di trattamento di dati personali. A tali soggetti viene attribuita la qualità di Responsabile esterno del trattamento dei dati personali ai sensi dell'articolo 28 del Regolamento UE 2016/679.
Agli accordi con le strutture accreditate e nei contratti di affidamento di fornitura o di servizi all'esterno dell'Azienda (outsourcing), nuovi o in essere, dovrà essere allegato un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, mediante il quale si vincola il responsabile del trattamento al titolare del trattamento e si disciplina il trattamento dei dati, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento così come previsto dall'art. 28 del Regolamento UE 2016/679.

in sede di prima applicazione del presente regolamento, le strutture aziendali competenti per la stipula e la conservazione dei contratti effettuano una ricognizione dei contratti in essere, al fine di provvedere all'eventuale nomina di Responsabile esterno del soggetto a cui è affidata l'attività o il servizio.
Le copie di tali contratti devono essere inviate alla Direzione Generale. I responsabili esterni operano nel rispetto del presente regolamento.

Articolo 8 — Autorizzato al Trattamento sotto l'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679
già Responsabile interno del trattamento dei dati personali

Ai sensi dell'articolo 29 del Regolamento UE 2016/679 "// *responsabile del trattamento, o chiunque agisca sotto la* sua *autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo* richiede *il diritto dell'Unione o degli Stati membri."*
L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro in qualità di titolare del trattamento dei dati individua i soggetti aziendali che agiscono sotto la sua autorità, che hanno accesso ai dati personali e che trattano tali dati secondo le sue istruzioni.
Per tali ragioni il titolare del trattamento mediante l'atto di autorizzazione al trattamento dei dati abilita i propri dipendenti a trattare i dati nell'ambito di detta organizzazione aziendale e per le finalità dalla stessa perseguite. Il trattamento effettuato dal soggetto non autorizzato non è

legittimo.
Il titolare del trattamento dei dati delibera la designazione dei suddetti soggetto e redige un atto di autorizzazione che contiene l'ambito del trattamento autorizzato e le istruzioni per il trattamento, per l'uso dei dispositivi e le misure di sicurezza da adottare.
Per quanto riguarda la designazione dei soggetti autorizzati al trattamento dei dati personali ai sensi dell'articolo 29 del Regolamento UE 2016/679 L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro delibera che ciò avverrà secondo due livelli, un primo livello che risponderà direttamente al titolare del trattamento dei dati comprendente:

I) figure apicali autorizzate quali:
a) il Direttore Amministrativo
b) il Direttore Sanitario Aziendale,
c) I direttori di SS.OO.CC.
d) I direttori di SS.OO.SS.DD.

II) un secondo livello che risponderà ai soggetti apicali autorizzati dicui al punto I di detto articolo comprendente:

III) a) soggetti autorizzati semplici.
IV) A tutti i dipendenti verrà inviata, mediante comunicazione, l'autorizzazione al trattamento, nella quale sarà indicato almeno l'ambito del trattamento per il quale sono autorizzati, il profilo utente rispetto alla rete aziendale, i corsi di formazione sulla protezione dei dati punto il regolamento impone l'obbligo di formazione del personale ex articolo o9 del Regolamento UE 2016/679.
V) I soggetti di cui al punto I del presente articolo compiono quanto necessario nel rispetto delle vigenti disposizioni in tema di riservatezza; in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate nel piano di sicurezza dei dati personali elaborato dall'Azienda.I soggetti di cui al punto I sono tenuti a:
VI) comunicare tempestivamente al Titolare del trattamento dei dati tutte le questioni rilevanti ai fini della normativa in materia di protezione dei dati personali;
VII) comunicare al Titolare del trattamento dei dati 1'inizio di ogni nuovo trattamento nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza,ai fine della compilazione dell'aggiornamento del registro dei trattamenti dei dati personali, nonché per quanto previsto ai sensi dell'articolo 4 ai numeri 6) e 7

Articolo 9 —Criteri per l'individuazione dei soggetti apicali autorizzati al Trattamentosotto l'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679

I soggetti apicali autorizzati al Trattamento sotto l'autorità del titolare del trattamento come previsto dall'art. 29 del Regolamento UE 2016/679 così come definiti ed indicati nell'articolo 8 del presente regolamento sono individuati fra i soggetti che per competenza ed esperienza, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
All'interno dell'Azienda sono indicati in coloro che ricoprono funzioni dirigenziali ed in

particolare:
Direttori di Struttura Complessa Direttori di strutture Dipartimentali altri dirigenti, per i quali si rende opportuna la designazione di autorizzati apicali al trattamento in virtù, delle particolarità organizzative e funzionali delle attività di competenza.
L'elenco completo dei soggetti apicali autorizzati è contenuto nella delibera di approvazione XXX Aziendale e disponibile presso XXC

Articolo 10 — Nomina dei soggetti autorizzati al Trattamento sotto 1'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679

La nomina dei soggetti apicali autorizzati al Trattamento sotto l'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679 viene effettuata con **atto deliberativo**.
L'atto di autorizzazione al trattamento dei dati dovrà essere comunicato per iscritto ai soggetti individuati.

Articolo 11 — Nomina dei soggetti autorizzati al Trattamento sotto l'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679 semplici

I soggetti autorizzati semplici (punto Il dell'articolo 8 del presente regolamento) sono identificati dai soggetti apicali autorizzati al Trattamento sotto l'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679 in tutti coloro che sono autorizzati ad effettuare operazioni di trattamento dei dati nell'ambito delle attività lavorative svolte in azienda.
Essi, in relazione alle funzioni loro assegnate, hanno accesso ai soli dati la cui conoscenza sia strettamente necessaria al trattamento.
Gli autorizzati semplici devono eseguire i trattamenti nel rispetto delle procedure secondo le disposizioni date dal soggetto autorizzato al Trattamento sotto l'autorità del titolare del trattamento ex art. 29 del Regolamento UE 2016/679 del trattamento, con nomina per iscritto.

Articolo 12 — Criteri per l'esecuzione del trattamento dei dati personali

L'Azienda garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.
La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale.
Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano come previsto dall'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea.
L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza. A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale aziendale e 1'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda. Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di

conseguenza dal presente nuovo Regolamento aziendale.

Parte III

Articolo 13 — Il registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (come previsto dall'articolo 30, paragrafo 5 del Regolamento UE 2016/679), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.
Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. Il Registro, in virtù delle dimensioni e della complessità che caratterizzano questa L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro , non può che avere forma elettronica.
La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.
Per tali spiegate ragioni ed in ottemperanza dei principi previsti dal Regolamento UE 2016/679 L'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro si è dotata di tale registro dei trattamenti in formato elettronico.
Per la compilazione del suddetto registro 1'Azienda ha realizzato un censimento dei trattamenti dei dati personali e/o sensibili (anagrafe). Il censimento contiene per ogni UU.OO. i trattamenti dei dati di competenza suddivisi per tipologie e per strutture organizzative, come presupposto necessario per adempiere agli obblighi del cennato Regolamento; è tenuto a cura del Titolare, in collaborazione con i soggetti apicali autorizzati al trattamento e vi sovrintende il Responsabile della Protezione dei dati; esso viene aggiornato qualora vengano comunicati da parte del Titolare o dei Responsabili del trattamento nonché dei soggetti apicali autorizzati al trattamento casi di attivazione, cessazione o modifica di nuovi trattamenti.

PARTE IV L'INTERESSATO

Articolo 14 — Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Come stabilito dall'articolo 13 del Regolamento UE 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.);

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, gli legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, 1'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare taleperiodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato su11'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se 1'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per 1'interessato. L'informativa rappresenta l'elemento propedeutico al trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere. Le predette informative vengono rese agli interessati anche tramite la pubblicazione sul sito aziendale nonché anche tramite l'affissione a stampa nei locali di accesso all'utenza e del personale aziendale.

Articolo 15 — Diritti dell'interessato

Secondo quanto disposto dal paragrafo III del Regolamento UE 2016/679 all'interessato ha diritto vengono riconosciuti i seguenti diritti:

- il diritto di accesso dell'interessato (articolo 15 Considerando 6o e Considerando 64)
- il diritto di rettifica (articolo 16 Considerando 65)

- il diritto alla cancellazione(c.d.diritto all'oblio" articolo 17 Considerando 65 e Considerando 66)
- il diritto di limitazione di trattamento (articolo 18 Considerando 67)
- il diritto alla portabilità dei dati (articolo 20 Considerando 68)
- il diritto di opposizione (articolo 21 Considerando 69 e Considerando70)

a) diritto di accesso dell'interessato

- Come stabilito dall'articolo 15 del Regolamento UE 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi l e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché 1'importanza e le conseguenze previste di tale trattamento per 1'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 del Regolamento UE 2016/679 relative al trasferimento. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se 1'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di accesso documentale", di accesso civico" e di "accesso generalizzato". Nel dare evidenza del fatto che, presso questa Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro , la competenza sulla materia de quo è affidata alla UU.OO. Affari Generali, si rinvia al contenuto delle schede informative pubblicate sul sito internet aziendale dedicate all'argomento.

A tale riguardo, nel rinviare a quanto pubblicato al sito web aziendale, si fa presente che:

a) per accesso documentale si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti dell'Azienda, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184).

Possono fare domanda tutti i cittadini portatori di un "interesse diretto, concreto e attuale corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso" (art. 22, Legge 241/1990). Per presentare domanda, è necessario rivolgersi alla

UU.OO. Affari Generali, portando con sé il proprio documento di identità valido. I costi di ricerca, visura e riproduzione fotostatica, e le spese di spedizione, sono quelle previste dal tariffario aziendale pubblicato sul sito web aziendale. Il procedimento di accesso si conclude entro 0 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).

b) **per accesso civico** si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone 1'obbligo (Decreto Legislativo 97 del 17/5/2016.

revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche", e Decreto Legislativo » del 14/03/2013: "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni").
La richiesta viene presentata alla UU.OO. Affari Generali utilizzando il modulo prodotto sul sito internet aziendale. L'Azienda, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, 1'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Azienda indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web aziendale) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.

c) per accesso generalizzato si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori

rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 (' Decreto Trasparenza') e del D.lgs. 97/2016 (così detto Freedom of Information Act o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico. La richiesta viene presentata alla UU.OO. Affari Generali utilizzando il modulo pubblicato sul sito internet aziendale. Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza, con la comunicazione dell'esito al richiedente e agli eventuali contro interessati. Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al contro interessato. Se il documento risulta già pubblicato nel sito aziendale nel rispetto della normativa vigente, l'Azienda indica al richiedente il relativo collegamento ipertestuale. Nei

casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni.

b) Diritto di rettifica

Come stabilito dall'articolo 16 del Regolamento UE 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

c) Diritto alla cancellazione "diritto all'oblio"

Come stabilito dall'articolo 17 del Regolamento UE 2016/679, in capo all'interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.
Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

d) Diritto alla limitazione al trattamento

Come previsto dall'articolo 18 del Regolamento UE 2016/679 in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi successivo punto f) del regolamento (in attesa della valutazione da parte del titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante). Il diritto alla limitazione prevede che il dato personale sia contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

e) Diritto alla portabilità dei dati

Come previsto dall'articolo 20 del Regolamento UE 2016/679. Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE). Inoltre, il Titolare deve essere in grado di trasferire

direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

f) Diritto di opposizione

Come stabilito dall'articolo 21 del Regolamento UE. 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.
Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

g) Processo decisionale automatizzato (Profilazione)

Come stabilito dall'articolo 22 del Regolamento UE 2016/679, 1'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o 1'esecuzione di un contratto tra 1'interessato e un titolare del trattamento; - sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato; - si basi sul consenso esplicito dell'interessato.

Parte VI Sicurezza

Articolo 14 — Amministratori di Sistema

Il Titolare e i Responsabili del trattamento per i quali si prevede l'utilizzo di apparecchiature informatiche si avvalgono, nella individuazione e applicazione delle misure necessarie a garantire la sicurezza del sistema, di amministratori di sistema formalmente individuati a tale scopo dal Responsabile del Servizio Sistema Informativo Aziendale ai sensi del
D.P.R. 318/99 e ss mm e ii, che deve essere nominato con apposito atto interno.

Articolo 15 - Sicurezza degli archivi cartacei

L'accesso agli archivi aziendali deve essere controllato, e devono essere identificati, autorizzati e registrati i soggetti.
Con riferimento agli archivi aziendali la responsabilità della conservazione e sicurezza dei medesimi spetta al responsabile competente per i dati oggetto del trattamento; i/il responsabili/e dovranno essere nominati con apposito atto deliberativo.
Gli archivi delle cartelle cliniche prodotte in ambito ospedaliero sono sotto la responsabilità:
del Direttore della U.O. (o del modulo dipartimentale) dal momento della formazione della cartella e per tutto il periodo di conservazione della medesima presso il reparto;
del Direttore del Presidio Ospedaliero al momento in cui la cartella perviene all'archivio centralizzato;
per le cartelle cliniche e la documentazione equipollente giacente presso strutture non ospedaliere la responsabilità farà capo al Direttore della Struttura ove i medesimi atti sono materialmente conservati;
nel caso di documentazione archiviata presso ditta convenzionata, il legale rappresentante della

medesima è responsabile della conservazione e della sicurezza;
nel contratto di affidamento del servizio dovrà essere prevista un'apposita clausola di garanzia e la possibilità per l'Azienda di accedere ai locali per verificare il rispetto alle prescrizioni della legge in materia di privacy e del presente regolamento.

Articolo 16 — Misure di sicurezza fisiche

Gli archivi cartacei devono essere situati in locali non esposti a rischi ambientali (quali allagamenti, incendi, deterioramenti di varia natura etc.), anche in ossequio alle disposizioni in materia di sicurezza di cui D. lgs 81/08 e successive modificazioni ed integrazioni.
E' opportuno che venga predisposto un piano periodico aziendale per la conservazione e lo scarto dei documenti, in conformità alle vigente normativa nazionale in tema di conservazione di documenti. A tal fine, partendo dalla rilevazione dei trattamenti di dati ai sensi del D. lgs 196/03 così come novellato dal D.Lgs.101/18, le singole strutture operative aziendali sono tenute a segnalare al DPO la tipologia, 1'ubicazione, il metodo di catalogazione e di custodia, la quantità approssimativa e 1'anno di riferimento della documentazione custodita ai fini dell'aggiornamento del censimento dei trattamenti di dati personali e/o sensibili.
Per la documentazione riguardante dati personali sensibili e non, è opportuno che ciascun presidio/edificio aziendale si dotasse di un proprio archivio centralizzato munito di misure di sicurezza (meccanismi di chiusura dei locali e dei contenitori, sistemi di allarme a protezione dei locali, etc..) idonee a garantire 1'inaccessibilità ai locali stessi da parte di soggetti non autorizzati.
Per quanto concerne specificatamente la documentazione sanitaria ed in particolare le cartelle cliniche, per le modalità di tenuta, archiviazione e rilascio copia ogni Azienda dovrà attenersi alla normativa vigente, prestando particolare attenzione a quanto stabilito nel1'Articolo 92 del D. Lgs.196/03 cosi come novellato dal D. Lgs. 101/18

Articolo 17 — Misure di sicurezza logiche

L'Azienda è tenuta ad impartire ai dipendenti che, in ragione delle loro mansioni si trovino ad utilizzare dati personali sensibili e non, adeguate raccomandazioni al fine di una doverosa responsabilizzazione dei soggetti stessi, in particolare per ciò che concerne la conservazione della documentazione cartacea onde evitare accessi non autorizzati perdita smarrimento o distruzione dei dati stessi.

Ricordando che la circolazione intraaziendale dei dati, in particolar' modo di quelli sensibili. non può eccedere quanto necessario per il puntuale svolgimento dei compiti istituzionali, si raccomanda all'Azienda di adottare modalità e accorgimenti tali da garantire il massimo rispetto della normativa contenuta nel Regolamento UE 2016/679 nonché nel D.lgs 196/2003 così come novellato dal D. Lgs. 101/18 soprattutto in relazione ai provvedimenti amministrativi, in particolare delibere e determina dirigenziali, in special modo nella fase di pubblicazione e di rilascio di copie ai sensi della L. 241/90 e s.m.i.

La sicurezza dei dati assicurata con le modalità qui disposte deve essere garantita anche per i dati

trattati da personale non dipendente del1'Azienda (tirocinanti, specializzandi.), nonché da personale dipendente che svolge

attività libero-professionale intramuraria nei casi in cui questa si svolga presso le strutture aziendali o comunque in focali messi a disposizione dell'Azienda.

Articolo 18 — Misure di sicurezza informatiche

Secondo quanto riportato nel regolamento per la sicurezza informatica, la cui elaborazione è a cura della Responsabile SIIA, si distinguono le seguenti tipologie di trattamento dei dati informatici:

- Trattamento dei dati su personal computer

Ciascun dipendente è responsabile del personal computer assegnato; l'Azienda anche con delega alle UU.OO. autorizzate ai trattamenti; ha predisposto idonee procedure di salvataggio periodico degli archivi e di antivirus, nonché a provvedere alla. registrazione degli accessi con assegnazione ed inserimento di password, tenendo sempre presente le misure adeguate di sicurezza previste dal Regolamento UE 2016/679.

- Trattamento dei dati all'interno di procedure inrete:

le apparecchiature informatiche devono essere collocate in locali non esposti a rischi ambientali (allagamenti, incendi, deterioramenti di varia natura...), anche in conformità alle disposizioni in materia di sicurezza di cui al D. lgs 81/2008;

i server devono essere posti sotto gruppo di continuità, onde evitare sbalzi o cadute di tensione che potrebbero danneggiare i dispositivi fisici delle macchine e quindi dei dati; deve essere previsto un sistema di salvataggio periodico sul data-base aziendale;

è opportuno che vengano previste modalità di autenticazione per l'accesso alle varie procedure (password, schede magnetiche, firma digitale, etc...); l'Azienda è tenuta a realizzare una propria rete che si interfacci verso l'esterno in maniera controllata e garantita da appositi meccanismi di difesa (proxy-server antivirus e firewall).

- Accessi ai dati

  Gli accessi vengono gestiti dal SIIA aziendale mediante credenziali personali:

- **Profile utenti**

i profili utenti assegnati rispecchiano compiti e mansioni assegnate.

Si raccomanda ai dipendenti il buon uso del proprio Sistema di lavoro che non dovrà mai essere utilizzato per fini personali.

- **Password**

La password di accesso alla postazione di lavoro nonché quelle di accesso agli applicative aziendali sono strettamente personali.

Logistica e software

È vietata qualsivoglia modifica logistica ed al software. Per fare ciò è necessario contattare il servizio all'uopo incaricato dall'azienda.

- **Disattivazione dell'utenza**

In caso di sospensione e/o cessazione dal rapporto di lavoro il servizio incaricato tramite la struttura CED provvederà ad annullare il relativo profilo utente e la password.

ARTICOLO 19— Videosorveglianza

L'Azienda disciplina L'attività di videosorveglianza finalizzata alla sicurezza degli utilizzatori, utenti o dipendenti, delle strutture aziendali, nonché alla tutela del patrimonio aziendale, con apposito regolamento pur nel pieno rispetto della normativa sulla privacy.
Non rientra nel campo di questa attività 1'utilizzo di apparecchiature strumentali per la rilevazione ed il monitoraggio dei parametri vitali dei pazienti né le attività di controllo a distanza dei lavoratori.
L attivazione di trattamenti di dati con modalità particolari tali da coinvolgere anche informazioni relative al personale dipendente (quali videosorveglianza, monitoraggio della posta elettronica e degli accessi a Internet etc.) L'Azienda adotterà una specifica regolamentazione atta a garantire il rispetto della normativa in tema di riservatezza dei dati personali nonché di tutela del lavoratore dipendente (Legge n. 300/70).
Simile regolamentazione sarà, altresì adottata per garantire lo scambio di notizie tra l'Azienda ed i mezzi ufficiali di informazione (giornali e televisioni), onde assicurare il massimo rispetto della riservatezza dei dati personali dei soggetti interessati dalie notizie e, contemporaneamente il diritto-dovere di informazione.
Come noto l'uso intensivo di dispositivi video influisce sul comportamento dei cittadini. Un ricorso significativo a tali strumenti in numerosi ambiti della vita delle persone eserciterà su queste ultime un'ulteriore pressione per impedire il rilevamento di quelle che potrebbero essere percepite come anomalie. Di fatto, queste tecnologie possono limitare le possibilità di muoversi e di utilizzare servizi in maniera anonima nonché, in linea generale, la possibilità di passare inosservati. Le conseguenze per la protezione dei dati sono enormi.
L'Azienda opera nel rispetto della normativa vigente e nello specifico delle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video Versione 2.0 Adottate il 29 gennaio 2020 da parte del Comitato europeo per la protezione dei dati (European Data Protection Board)

ARTICOLO 21- PROVVEDIMENTO GARANTE PROTEZIONE DEI DATI DEL 7 MARZO 2019

L'emergenza COVID -19 ha ribadito la centralità della disciplina della protezione dei dati personali; nello specifico a raccolta e l'utilizzo dei dati, in particolare quelli relativi alla salute, si è rivelata strumento indispensabile nell'azione di contrasto della pandemia. Per quanto riguarda il trattamento di "categorie particolari di dati personali" (art. 9 del Regolamento UE 2016/679 cd GDPR) – tra i quali

rientrano i dati relativi alla salute – esso è, in via generale, vietato a meno che il titolare dimostri di soddisfare almeno una delle condizioni previste dall'art. 9, par. 2 del medesimo regolamento. Il divieto generale di trattare le "categorie particolari di dati", tra cui anche quelli sulla salute, consente alcune deroghe, che rendono lecito il trattamento di tali dati. Nel caso che ci riguarda le eccezioni, previste dal paragrafo II dell'art. 9 del Regolamento, sono riconducibili ai trattamenti necessari per: lettera g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (cd finalità di interesse pubblico) lettera h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (cd finalità di diagnosi, assistenza e terapia) , il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (cd finalità di sanità pubblica e di protezione da gravi minacce per la salute a carattere transfrontaliero).

Tale impostazione viene confermata dal novellato codice privacy all'articolo 75.

Per tali spiegate ragioni i trattamenti di dati effettuati per finalità determinate e connesse alla cura della salute ed effettuati da un professionista sanitario soggetto al segreto professionale (o altra persona soggetta all'obbligo di segretezza), non richiedono il consenso dell'interessato al trattamento dei dati.

Si rappresenta, inoltre, che non rientrano nelle ipotesi sopra richiamate e che richiedono ancora il consenso esplicito dell'interessato (art. 9, par. 2, lett. a), quei trattamenti connessi all'utilizzo di App mediche – con le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato. Si ribadisce, altresì, che rimane invariato l'obbligo di rendere al paziente in forma chiara l'informativa ai sensi dell'articolo 13 e 14 del cennato Regolamento. Si specifica, infine, che tali indicazioni e tutto ciò che è connesso con le novità legislative in tema di protezione del dato saranno oggetto di attività di istruzione e formazione aziendale non appena le condizioni pandemiche lo permetteranno

ARTICOLO 22- SMARTWORKING

A causa dell'epidemia di coronavirus **l'Azienda Ospedaliera "Pugliese Ciaccio" di Catanzaro** , quale **titolare del trattamento**, ha incentivato Lo smart working , in particolare il personale amministrativo e di staff.

Lo smartworking pone rilevanti questioni sotto il profilo privacy, considerando i possibili rischi. Infatti, in base a quanto disposto dal GDPR, l'Azienda ha messo in atto misure tecniche e organizzative, idonee a garantire un livello di sicurezza dei dati trattati adeguato al rischio e gravità, il Titolare del trattamento adotta politiche ed attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme allo stesso GDPR. Questo significa non solo divenire responsabile delle scelte di mezzi, operazioni, procedure, finalità in materia di trattamento dei dati, ma anche **essere in grado di "dare conto" delle valutazioni svolte alla base delle scelte operate.**

Con riferimento allo *smart working*, il principio di *accountability* si estende a qualsiasi iniziativa o misura intesa a favore i trattamenti di dati da svolgersi in modalità di *smart working* e ciò implica il porre in essere di **comportamenti proattivi**, che dimostrino la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR.

Spetta al Titolare, quindi, decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce dei criteri specifici indicati nel GDPR. Nella pratica, il Titolare deve:

- integrare il registro dei trattamenti, da tenersi ai sensi dell'art. 30 GDPR, con nuovi elementi (trattamenti, banche dati, strumenti, esternalizzazioni, misure di sicurezza) che dovessero riguardare le attività in smart working; questi elementi saranno utili anche per formulare pareri professionali sulla materia;
- valutare, in base a quanto disposto nel GDPR e nello **Statuto dei Lavoratori** il potenziale invasivo di eventuali sistemi, che consentano il monitoraggio dell'utilizzo degli strumenti e della "rete aziendale", eventualmente sottoponendoli a valutazione d'impatto – DPIA ex 33 GDPR;
- valutare la necessità di integrare l'informativa ai lavoratori, in virtù di eventuali nuovi trattamenti datoriali collegati allo smart working;
- integrare o riformulare, in funzione del contesto delocalizzato, le istruzioni per la sicurezza dei dati da rendersi allo smart worker;

- intraprendere specifiche iniziative di formazione per fornire allo stesso gli opportuni strumenti di conoscenza e consapevolezza;
- ampliare, se necessario, l'ambito di autorizzazione degli amministratori di sistema;
- verificare che le soluzioni informatiche eventualmente sviluppate internamente per consentire lo svolgimento del lavoro a distanza siano conformi ai principi di **privacy by design/by default** e garantiscano la sicurezza dei dati ex 32 GPDR;
- verificare la contrattualistica e la conformità al GDPR delle soluzioni o piattaforme fornite da terzi (ad esempio, per il networking), valutando la necessità e l'adeguatezza di eventuali data processing agreement da sottoscrivere ai sensi dell'art. 28 del GDPR per la nomina a Responsabili del trattamento.

Il Titolare del trattamento deve informare i lavoratori, nonché i professionisti facenti parte di uno studio professionale in *smart working* su quale sia l'ambito di trattamento consentito. Gli stessi saranno autorizzati ad eseguire i medesimi trattamenti di dati, che sono ammessi a svolgere in ufficio o presso lo studio professionale secondo le proprie mansioni, fatte salve le attività non eseguibili da remoto, nonché le diverse e specifiche indicazioni del Datore di lavoro, correlate alla diversa modalità di operare. Parimenti, è opportuno che il Titolare **ribadisca al personale ed ai professionisti in *smart working* che essi sono tenuti ad attenersi**, qualora compatibili ed e applicabili al contesto "extra aziendale", **alle medesime istruzioni** e procedure già rese dal Titolare in tema di trattamento e tenuta in sicurezza dei dati personali. Pertanto, è necessario che il Titolare informi i lavoratori ed i professionisti che anche in caso di prestazioni rese a distanza, permangono e, quindi, vigono gli obblighi generali di:

- non violare il segreto e la riservatezza delle informazioni trattate;
- proteggere i dati contro i rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito;
- rispettare e applicare le misure di sicurezza fisiche, informatiche, organizzative, logistiche e procedurali;
- utilizzare soltanto per rendere la prestazione lavorativa gli eventuali strumenti tecnologici "aziendali", quali *computer*, *smartphone*, ecc., che il Titolare abbia concesso in uso anche al di fuori della struttura;
- contattare il Titolare o l'amministratore di sistema per qualsiasi dubbio, sospetto di incidente o di violazione che possa compromettere i dati aziendali o dello studio professionale.

Inoltre, gli *smart worker* devono essere informati dal Titolare della necessità di adottare specifiche cautele in relazione alla propria postazione di lavoro. La finalità è quella di specificare in relazione al

contesto i principi di **preservazione della riservatezza e dell'integrità** delle informazioni aziendali, tracui rientrano i dati personali trattati in esecuzione delle proprie mansioni, in quanto per molti lavoratori può porsi il problema della promiscuità, aspetto questo che è risultato particolarmente evidente durante il l*ockdown* quando gran parte di noi si è trovata a lavorare in uno stato di costante contiguità coi propri familiari.

A) La protezione degli strumenti personali usati per lavorare

Qualora il lavoratore o il collaboratore non disponga di un dispositivo "aziendale" o fornito dallo studio professionale ed utilizzi **un dispositivo personale** per eseguire la prestazione lavorativa, deve aver curadi:

- utilizzare un dispositivo, se possibile, ad uso esclusivo personale;
- creare **un account personale** nel caso in cui il dispositivo sia ad uso condiviso con i familiari e in modo che il lavoratore acceda ad una partizione a suo uso esclusivo;
- proteggere l'accesso al dispositivo (o alla propria partizione) con credenziali conosciute soltanto del lavoratore, evitando qualsiasi forma di condivisione;
- evitare il ricorso a credenziali facilmente intuibili o ricostruibili;
- verificare che il dispositivo sia aggiornato quanto a misure di protezione, quali *antivirus*, *antimalware*, e *firewall* e a tal fine il Datore di lavoro dovrà indicare i *tool*di sicurezza più adatti;
- verificare che il *device*sia aggiornato con l'ultima versione disponibile del sistema operativo su cui gira;
- non salvare i "documenti aziendali" nella memoria del proprio dispositivo o in altre periferiche personali laddove siano disponibili funzioni di salvataggio su server aziendali;
- non aprire allegati o *link* che destino sospetti;
- **non scaricare programmi di dubbia provenienza**;
- disconnettersi accuratamente a fine sessione dagli applicativi aziendali.

B) Protezione del dispositivo di lavoro aziendale

Con riguardo ai **dispositivi di lavoro forniti dal Titolare**, lo strumento dovrebbe essere già predisposto, quanto a sicurezza, delle informazioni tramite dotazione di:

- sistema operativo aggiornato; misure di protezione da intrusioni (*antivirus*, *firewall*, *patch* di sicurezza) aggiornate. Il lavoratore o il professionista dovrà essere comunque chiamato a scaricare gli opportuni aggiornamenti, laddove il Datore di lavoro non abbia implementato automatismi a riguardo.
- tecniche di cifratura;
- eventuale blocco delle porte USB e di connettori ad altre periferiche;
- configurazione dell'accesso remoto ai sistemi aziendali;
- configurazione del pacchetto di applicativi autorizzati;
- *tool script* di back-up automatizzato su server aziendale.

ARTICOLO 23 - Norma di rinvio

Per quanto non espressamente disciplinato dal presente Regolamento si rimanda al Regolamento UE 2016/679 nonché quanto previsto dal D. Lgs. 196/03, 101/2018 e successive modificazioni ed integrazioni.

Allegato-1 SOGGETTI APICALI AUTORIZZATI AL TRATTAMENTO DEI DATI

U.O. NOME	RESPONSABILE
DIRETTORE AMMINISTRATIVO	AVV. ANTONIO MANTELLA
Referente SANITARIO AZIENDALE	DR. SERGIO PETRILLO
SOC AFFARI GENERALI	AVV. ANTONELLA CIAMPA
SOC GESTIONE ECONOMICO FINANZIARIO	AVV. WALTER TALARICO
SOC ATTIVITA' TECNICHE	- AD INTERIM WALTER TALLERICO
SOC Acquisizione Beni e servizi	FF AVV. PAOLO TRIPODI
SOC GESTIONE RISORSE UMANE	FF AVV. LAURA FONDACARO
S.O.S . AFFARI LEGALI	DOTT. FLORENZA RUSSO
SOS. URP	DOTT.DOMENICO CANINO
SOC NEFROLOGIA E DIALISI	DOTT.SALVATORE CHIARELLA
SOC GERIATRIA	DOTT. GIOVANNI RUOTOLO
SOC GASTROENTEROLOGIA ED ENDOSCOPIA DIGESTIVA	DOTT. STEFANO RODINO

SOC MALATTIE ENDOCRINE DEL RICAMBIO E NUTRIZIONE	DOTT. LUGI PUCCIO
SOC . DERMATOLOGIA	DOTT. GIANCARLO VALENTI
SOC. MEDICINA GENERALE	DOTT. CARMELO PINTAUDI
SOC .MALATTIE INFETTIVE	DOTT. LUCIO COSCO
SOC. CHIRURGIA GENERALE	DOTT. ROSARIO CARDONA
SOC CHIRURGIA PLASTICA	DOTT. FRANCESCO ABBONANTE
SOC CHIRURGIA VASCOLARE	DOTT. PAOLO RUBINO
SOC ENDOSCOPIA CHIRURGICA OPERATIVA	DOTT. DARIO BAVA
SOC ORTOPEDIA E TRAUMATOLOGIA	DOTT. VICENZO MACRI
SOC UROLOGIA	FF DOTT MICHELE PRINCIPE.
SOSD CHIRURGIA D'URGENZA	DOTT. NICOLA DE GRAZIA
SOSD DAY SURGERY AUTONOMO MULTIDISCIPLINARE	DOTT. ALFONSO CIACCI
SOC EMATOLOGIA	DOTT. MARCO ROSSI
SOC EMATOLOGIA ED ONCOLOGIA PEDIATRICA	DOTT. MARIA CONCETTA GALATI
SOC EMOFILIA E PATOLOGIE DELLA COAGULAZIONE	DOTT.RITA CARLOTTA SANTORO
SOC ONCOLOGIA MEDICA	DOTT. VITO BARBERI
SOC RADIOTERAPIA ONCOLOGICA E RADIOBIOLOGIA	DOTT. .SSA ELVIRA MAZZEI
SOC SERVIZIO DI IMMUNOEMATOLOGIA E MEDICINA TRASFUSIONALE	DOTT. SSA GABRIELLA TALARICO
SOD CURE PALLIATIVE	DOTT. ROBERTO SQUILLACE
SOC ANESTESIA E RIANIMAZIONE	DOTT. MARIA LAURA GUZZO
SOC CARDIOLOGIA - UTIC - EMODINAMICA	DOTT. VINCENZO ANTONIO CICONTE

SOC MEDICINA D'URGENZA ED ACCETTAZIONE	DOTT. PEPINO MASCIARI
SOC CHIRURGIA PEDIATRICA	DOTT. DOMENICO SALERNO
SOC NEONATOLOGIA E TERAPIA INTENSIVA NEONATALE	DOTT. MARIA LUCENTE
SOC OSTETRICIA E GINECOLOGIA OSPEDALIERA	FF DOTT. MINOTTI PULLANO
SO SD OSTETRICIA E GINECOLOGIA OSPEDALIERA PMA	DOTT. ROBERTA VENTURELLA
SOC OSTETRICIA E GINECOLOGIA UNIVERSITARIA	DOTT. FULVIO ZULLO
SOC PEDIATRIA OSPEDALIERA	DOTT. GIUSEPPE RAIOLA
SOC PEDIATRIA UNIVERSITARIA	DOTT. DANIELA CONCOLINO
SOD CHIRURGIA ORALE	DOTT. SALVATORE DE FILIPPO
SOC NEUROCHIRURGIA	DOTT. GIUSEPPE MAURO
SOC NEUROLOGIA	DOTT. DOMENICO BOSCO
SOC OCULISTICA	DOTT. MAURIZIO POSTORINO
SOC ODONTOSTOMATOLOGIA E CHIRURGIA MAXILLO-FACCIALE	DOTT. ROMEO CARNEVALI
SOC OTORINOLARINGOIATRIA	DOTT. DESTITO DOMENICO
SOC ANATOMIA PATOLOGICA	DOTT. LUIGI TUCCI
SOC FARMACIA	DOTT.SSA. RITA MORILLO
SOC FISICA SANITARIA	DOTT.SSA. ANTONELLA ANOJA
SOC LABORATORIO CHIMICA CLINICA	DOTT. PIETRO GANGEMI
SOC LABORATORIO VIROLOGIA E MICROBIOLOGIA	DOTT. PASQUALE MINCHELLA
SOC MEDICINA FISICA E RIABILITATIVA	DOTT.SSA PAOLA BELMONTE
SOC MEDICINA NUCLEARE	DOTT. PAOLO PUNTIERI
SOC RADIOLOGIA DIAGNOSTICA	DOTT. BERNARDO BERTUCCI
SOD RADIOLOGIA DE LELLIS	DOTT. GIUSEPPE FODARO

SOC AREA PROGRAMMAZIONE E CONTROLLO	DOTT. SEGIO PETRILLO
SOD ATTIVITA' LIBERO PROFESSIONALE	DOTT. LUIGI MANCUSO
SOD RISK MANAGEMENT risk manager	DOTT. SSA MARIKA BIAMONTE
SOS SERVIZIO ISPETTIVO DI VERIFICA E CONTROLLO	DOTT. SSA DONATELLA PORCELLI
SOD COORDINAMENTO GOVERNO CLINICO	DOTT. GIUSEPPE PANELLA
SOS INGEGNERIA BIOMEDICA	ING. LUIGI SANTAGUIDA
UOC DIREZIONE MEDICA DE PRESIDIO - PUGLIESE	DOTT. GIANLUCA RAFFAELE
SOD DIREZIONE MEDICA DE PRESIDIO – DE LELLIS	DOTT. FRANCESCO TALARICO
AMMINISTRATORE DEL SISTEMA	DOTT. PIER RAFFAELE MARTORELLI
RESPONSABILE SISTEMI INFORMATIVI AZIENDALE	DOTT.SERGIO PETRILLO
RESPONSABILE TRASPARENZA PREVENZIONE DELLA CORRUZIONE	DOTT.SSA CATERINA FERRARO
RSPP	DOTT.SSA FILOMENA DE FRANCESCO
RESPONSABILE SITO WEB AZIENDALE	ING. TOMMASO CALIGIURI
RESPONSABILE ARCHIVIO CARTACEO	DOTT. MOLE' ANTONIO
MEDICO COMPETENTE	DOTT.SSA ROSA MAURO
MEDICO COMPETENTE	DOTT. ENRICO CIACCIO
MEDICO AUTORIZZATO	DOTT. VALERIA PUTRONE

ALLEGATO n. 1

Azienda Ospedaliera Pugliese Ciaccio

Egregio
Dr.

Direttore SOC /SOD
dell'A.O. Pugliese Ciaccio
88100 CATANZARO

OGGETTO: Nomina a Responsabile del Trattamento dei dati - Unità Operativa di **Struttura Complessa .....**Pugliese Ciaccio di Catanzaro.

L'Avv. Francesco Procopio, Commissario Straordinario, in qualità di "Titolare del Trattamento" dei dati personali, dell'Azienda Ospedaliera Pugliese Ciaccio di Catanzaro, conformemente a quanto stabilito dal GDPR (UE 2016/679) e dal D. Lgs. 10.08.2018 n. 101

AFFIDA

Al Dr……Direttore Struttura Complessa .....nominato con delibera n°……Direttore struttura complessa .....la mansione di Responsabile del Trattamento dei dati, con l'incarico di realizzare il sistema di sicurezza e di **accountability** per la Privacy dell'Unità Operativa di, **Struttura Complessa .....**in base alle scelte e regole contenute nell'Allegato "delega al responsabile del trattamento dei dati personali" in calce riportata.
Ai fini suddetti il responsabile del trattamento dei dati personali **dovrà**, nella propria Unità Organizzativa:
individuare le **persone che sono autorizzate al trattamento dei dati** per le attività in oggetto e ad esse afferenti;
coordinare e controllare l'adeguamento al GDPR delle persone che sono coinvolte nelle attività di gestione della suddetta UO, per mezzo di audit periodici;
curare la la responsabilizzazione di tutto il personale facente parte dell'U.O. Con la presente si rammenta l'importanza che la SOC di **Struttura Complessa .....**dotata di uno o più soggetti interni - di supporto al Titolare dei dati per il trattamento degli stessi in totale accordo col nuovo Regolamento europeo UE 2016/679. Sarà, pertanto, compito del Responsabile del Trattamento dei dati assicurarsi che

tutte le risorse interne e facenti parte dell'Unità Organizzativa attuino le regole di sicurezza e abbiano preso parte ai corsi di formazione sul nuovo regolamento europeo UE 2016/679. Il "Responsabile del Trattamento" dichiara di essere a conoscenza di quanto stabilito dal GDPR (UE 2016/679) per l'adozione delle misure di sicurezza, nonché del D. Lgs. 196/03 e del D. Lgs. 101/18 e si impegna ad attuare le norme in esso contenute.

Il Commissario Straordinario –
Titolare del trattamento

Il Responsabile del trattamento
Dr.

TRATTAMENTO DEI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, dovrà essere richiesta almeno l'osservanza delle seguenti modalità finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento, da parte degli incaricati, nelle operazioni di trattamento, degli atti e dei documenti contenenti dati personali:

- **individuare le persone che sono autorizzate al trattamento dei dati personali** e che afferiscono **Struttura Complessa ……..**alla predisporre la lista delle persone che sono autorizzate al trattamento e dei relativi profili di autorizzazione. Per ogni persona autorizzata occorre definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale (o inferiore se ne ricorre il caso) all'aggiornamento della lista e delle conseguenti autorizzazioni: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati al trattamento, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;
- quando **gli atti e i documenti contenenti dati personali indicati all'art. 9 del GDPR (UE 2016/679) (intesi come sensibili o giudiziari)** saranno affidati per lo svolgimento dei relativi compiti, i medesimi atti e documenti e **dovranno essere controllati e custoditi dalle persone che sono autorizzate al trattamento** fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e, al termine delle operazioni affidate, dovranno essere da questi restituiti;
- **l'accesso agli archivi contenenti dati di cui all'art. 9 del GDPR dovrà essere controllato**. Qualora le persone che sono autorizzate al trattamento di dati personali dovessero trattare documenti contenenti dati personali sensibili o giudiziari e per far ciò dovessero accedere all'archivio, gli stessi dovranno aver cura di esibire la documentazione comprovante l'autorizzazione all'accesso e al trattamento. Nel caso in cui le persone che sono autorizzate al trattamento fossero ammesse, a qualunque titolo, dopo l'orario di chiusura, dovranno dare le loro generalità in quanto vi è l'obbligo di identificare e registrare coloro che accedono agli archivi stessi. Qualora gli archivi non fossero dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, gli incaricati dovranno richiedere preventivamente l'autorizzazione all'accesso.

TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti elettronici, dovrà essere richiesta almeno l'osservanza delle modalità di seguito indicate.

Sistema di autenticazione informatica.

Individuare le persone che sono autorizzate al trattamento dei dati personali e predisporre la lista delle persone autorizzate che potrà essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. **Per ogni persona autorizzata al trattamento,** occorre definire **l'ambito del trattamento consentito e i relativi profili di autorizzazione**. Provvedere con cadenza almeno annuale (o inferiore se ne ricorre il caso) all'aggiornamento della lista e delle conseguenti autorizzazioni: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati, la lista delle persone che sono autorizzate al trattamento può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Il trattamento di dati personali con strumenti elettronici deve essere consentito alle persone autorizzate e dotate di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un

insieme di trattamenti. **Per le credenziali occorrerà osservare quanto disposto dal D. Lgs. 30.6.2003 n. 196, GDPR (UE 2016/679) e dal D. Lgs. 101/18.**
Ad ogni persona autorizzata devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.
Dovranno essere impartite, alle persone autorizzate, istruzioni per adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
Deve essere previsto che:
- le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica**;**
- le credenziali dovranno essere disattivate anche **in caso di perdita della qualità** che consente alla persona autorizzata l'accesso ai dati personali.
Devono essere impartite istruzioni alle persone autorizzate al trattamento, per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
Per i casi in cui l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, saranno impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può
assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto le persona autorizzata della loro custodia, la quale deve informare tempestivamente la persona autorizzata al trattamento, dell'intervento effettuato.
Sistema di autorizzazione
Nei casi in cui, per le persone autorizzate, siano individuati profili di autorizzazione di ambito diverso dovrà essere operativo un sistema di autorizzazione.
I profili di autorizzazione, per ciascuna persona autorizzata o per classi omogenee di persone autorizzate, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque almeno annualmente, dovrà essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione (o inferiore se ne ricorre il caso).
Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito alle persone autorizzate e addette alla gestione o alla manutenzione degli strumenti elettronici, la lista delle persone autorizzate può essere redatta anche per classi omogenee di persone autorizzate al trattamento e dei relativi profili di autorizzazione.
I dati personali dovranno essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare ogni qualvolta vengano resi disponibili gli aggiornamenti.
Dovranno essere effettuati aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.
Dovranno essere impartite istruzioni organizzative e tecniche per il salvataggio dei dati, con ragionevole frequenza, soprattutto sui singoli PC che non siano collegati ad un Server, o che, comunque, lavorino in modalità stand alone..

In modo da assicurare la dovuta padronanza di tutti i dipendenti delle Policy del Disaster Recovery e della Business Continuity **da regolamentare con l'Amministratore di Sistema e di concerto col DPO (fino alla realizzazione, di una Policy di Cloud)**.
Il responsabile del Trattamento dei dati dovrà avviare una elevata collaborazione col DPO, che dovrà curare la tenuta di un Registro dei Trattamenti, gli adempimenti di Data Breach, in seno ai dati trattati e fungere da interfaccia con la Struttura Garante.
Il calcolo dei Rischi, effettuato dal DPO, sarà attuato in collaborazione con tutti i Responsabili del Trattamento (32 del regolamento europeo).
Periodicamente **il DPO verificherà**, con audit interni, **il perfetto andamento delle Policy** impartite redigendo dei verbali, da sottoporre al Titolare dei dati, indicanti l'andamento delle direttive, con cadenza almeno bimestrale, che consentano una piena attuazione del GDPR.
Trimestralmente il DPO convocherà tutti i Responsabili del Trattamento al fine di rendere più performante le attività di trattamento. **Ogni *Incident* di sicurezza dovrà essere reso noto all'intera struttura**, per il tramite del DPO, per mezzo di comunicazioni ufficiali mirate alla minimizzazione del rischio.
Dovendo **il Responsabile del Trattamento dei dati coordinare la Struttura Complessa** , avrà l'onere di consegnare la Lettera di nomina alle persone autorizzate del trattamento dei dati che operano sui dati della dell'AOPC di CZ della UO indicata.
Responsabilità del Trattamento dei dati
Il Responsabile del trattamento ai sensi dell'art. 28 del GDPR (UE 2016/679) dovrà garantire le misure di sicurezza tecniche ed organizzative adeguate non inferiori a quelle richieste dall'art.32 del UE 2016/679 e sotto riportate: la pseudonimizzazione dei dati personali la cifratura dei dati personali;
la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. una procedura di valutazione dell'adeguato livello di sicurezza, che tenga conto in speciale modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
una procedura che definisca che chiunque operi sotto la sua autorità abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. l'adesione a un codice di condotta o a un meccanismo di certificazione approvati ai sensi della normativa pro tempore applicabile.

responsabilità e nell'ambito del proprio assetto organizzativo del Responsabile del trattamento

Catanzaro, __ / __ / _____
A: _____

OGGETTO: Lettera di nomina alla persona autorizzata al trattamento dei dati dell'Area dell'Unità Organizzativa dell'UO _____.

La presente per comunicarLe che nell'esecuzione della sua attività lavorativa esegue trattamenti di dati personali e prende visione di documenti che contengono i dati stessi. La normativa sulla Privacy, già col D. Lgs. 30.6.2003 n. 196 ed il nuovo GDPR (UE 2016/679), ha disposto che il personale che presta l'attività a favore del titolare o del Responsabile del trattamento può accedere ai dati personali, se autorizzato al trattamento per iscritto, a compiere le operazioni stesse del trattamento dal Responsabile del trattamento e sempre che operi sotto la diretta autorità, attenendosi alle istruzioni da questi impartite (ex art.30 D. Lgs. 30.6.2003 n. 196) e recepite nell'art. 2- quaterdecies del D. Lgs. 101/18. Lo scrivente, quindi, in qualità di Responsabile del Trattamento dei dati personali, conformemente a quanto stabilito dal D. Lgs. 10.08.2018 n. 101 (art. 2-quaterdecies) conferma che nello svolgimento della sua attività potrà trattare: a) i dati di cui all'art. 9 del GDPR contenuti nei documenti che deve utilizzare nello svolgimento delle attività nell'unità organizzativa ad essa afferente e ad accedere ai relativi archivi; b) i dati di cui all'art. 9 del GDPR di cui all'area suddetta contenuti in archivi e in strumenti elettronici utilizzando gli strumenti stessi; Nell'effettuare il trattamento dei dati, devono essere soddisfatti i principi della normativa vigente in materia di trattamento dei dati; infatti, i dati di cui alle lettere a) e b) devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, devono essere esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e la loro conservazione nella forma che consenta l'identificazione dell'interessato deve avvenire per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Nello svolgimento delle sue mansioni voglia adottare idonee misure di custodia e di controllo ed in genere qualunque accorgimento che consenta di ridurre al minimo i rischi di distruzione o perdita, anche accidentale di dei dati stessi e che consenta di ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e voglia osservare le procedure appositamente approntate per evitare quanto detto. Precisiamo che dovrà seguire, direttamente o coadiuvato da personale esperto se le attività sono di pertinenza del settore informatico, le particolari regole di sicurezza specificamente previste per la protezione contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale (antiVirus, antiWorm, protezione da programmi maligni in genere), per l'aggiornamento dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti per curare, almeno settimanalmente, il salvataggio dei dati seguendo le istruzioni organizzative e tecniche che abbiamo impartito con appositi incarichi (si veda l'Allegato

REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI).
Le ricordiamo che la normativa vigente, prevede particolari regole alle quali ogni persona

autorizzata al trattamento dovrà attenersi; regole che vengono riportate nell'Allegato REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI e che dovranno da Lei essere osservate. Il Responsabile del trattamento L'Incaricato del trattamento "
ALLEGATO REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI TRATTAMENTO DEI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, dovrà essere richiesta almeno l'osservanza delle seguenti modalità finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento, da parte degli incaricati, nelle operazioni di trattamento, degli atti e dei documenti contenenti dati personali: - individuare le persone autorizzate al trattamento dei dati personali e predisporre la lista delle persone autorizzate che potrà essere redatta anche per classi omogenee di autorizzazione al trattamento e dei relativi profili di autorizzazione. Per ogni persona autorizzata al trattamento definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale all'aggiornamento della lista e delle conseguenti autorizzazioni: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito alle singole persone autorizzate, la lista delle persone autorizzate può essere redatta anche per classi omogenee di autorizzazione al trattamento e dei relativi profili di autorizzazione; - quando gli atti e i documenti contenenti dati particolari indicati nell'art. 9 – 10 del GDPR (UE 2016/679) (già individuati dal D. Lgs. 196/03 come dati personali sensibili o giudiziari) saranno affidati per lo svolgimento dei relativi compiti, i medesimi atti e documenti dovranno essere controllati e custoditi dalle persone autorizzate fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e, al termine delle operazioni affidate, dovranno essere da questi restituiti; - l'accesso agli archivi contenenti dati sensibili o giudiziari dovrà essere controllato. Qualora le persone autorizzate al trattamento di dati personali dovessero trattare documenti contenenti dati personali particolari (sensibili o giudiziari) e per far ciò dovessero accedere all'archivio, le stesse dovranno aver cura di esibire la documentazione comprovante l'autorizzazione all'accesso e al trattamento. Nel caso in cui le persone autorizzate fossero ammesse, a qualunque titolo, dopo l'orario di chiusura, dovranno dare le loro generalità in quanto vi è l'obbligo di identificare e registrare coloro che accedono agli archivi stessi. Qualora gli archivi non fossero dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone autorizzate dovranno richiedere preventivamente l'autorizzazione all'accesso
TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI
Per il trattamento di dati personali, effettuato con strumenti elettronici, dovrà essere richiesta almeno l'osservanza delle modalità di seguito indicate. Sistema di autenticazione informatica. Individuare le persone autorizzate al trattamento dei dati personali predisporre la lista delle persone autorizzate che potrà essere redatta anche per classi omogenee di autorizzazione al trattamento e dei relativi profili di autorizzazione. Per ogni persona autorizzata definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale all'aggiornamento della lista e delle conseguenti autorizzazioni: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito alle singole persone autorizzate, la lista delle persone autorizzate può essere redatta anche per classi omogenee di autorizzazione al trattamento e dei relativi profili di autorizzazione.
Il trattamento di dati personali con strumenti elettronici deve essere consentito alle persone autorizzate dotate di credenziali di autenticazione che consentano il superamento di una

procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Per le credenziali occorrerà osservare quanto già disposto dal D. Lgs. 196/03. Ad ogni persona autorizzata devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione. Dovranno essere impartite alle persone autorizzate istruzioni per adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo della persona autorizzata. Deve essere previsto che: - le credenziali di autenticazione non utilizzate da almeno sei mesi dovranno essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; - le credenziali dovranno essere disattivate anche in caso di perdita della qualità che consente alla persona autorizzata l'accesso ai dati personali. Devono essere impartite istruzioni persone autorizzate per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Per i casi in cui l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, saranno impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento della persona autorizzata che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto le persone autorizzate della loro custodia, le quali devono informare tempestivamente la persona autorizzata al trattamento dell'intervento effettuato. Sistema di autorizzazione Nei casi in cui, per le persone autorizzate, saranno individuati profili di autorizzazione di ambito diverso dovrà essere operativo un sistema di autorizzazione. I profili di autorizzazione, per ciascuna persona autorizzata o per classi omogenee di persone autorizzate, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, dovrà essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. Sarà cura del Responsabile del Trattamento assicurarsi, anche per mezzo di personale di sua fiducia e afferente all'Unità Organizzativa, che, alla bisogna, ad ogni utente venga fatto firmare il modulo di consenso contenente le informazioni di cui agli art. 13 e 14 del Regolamento UE 2016/679 su come saranno trattati i dati di ogni interessato che si avvale dei servizi dell'Azienda, con l'esercizio degli artt. 16, 17, 18 e 21 nonché dell'art. 7 del GDPR. Il consenso sarà custodito diligentemente. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito alle singole persone autorizzate e addette alla gestione o alla manutenzione degli strumenti elettronici, la lista persone autorizzate può essere redatta anche per classi omogenee di autorizzazioni al trattamento e dei relativi profili di autorizzazione. I dati personali dovranno essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare ogni qualvolta vengano resi disponibili gli aggiornamenti. Dovranno essere effettuati aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti. Dovranno essere impartite istruzioni organizzative e tecniche sull'applicazione delle misure di sicurezza nonché per il salvataggio dei dati, soprattutto sui singoli PC che non siano collegati ad un Server. In modo da assicurare la dovuta padronanza di tutti i dipendenti delle Policy del Disaster Recovery e della Business Continuity da regolamentare con l'Amministratore di Sistema aziendale e di concerto col DPO. Il responsabile del Trattamento dei dati dovrà

avviare una elevata collaborazione col DPO Aziendale che dovrà curare la tenuta di un Registro dei Trattamenti, gli adempimenti di data Breach e fungere da interfaccia con la Struttura Garante. Il calcolo dei Rischi, attuato dal DPO, sarà effettuato in collaborazione con tutti i Responsabili del Trattamento in sinergia con l'art. 32 del regolamento europeo. Periodicamente il DPO verificherà, con audit interni, il perfetto andamento delle Policy impartite redigendo dei verbali, da sottoporre al Titolare dei dati, indicanti l'andamento delle direttive, con cadenza almeno bimestrale, che consentano una piena attuazione del GDPR.
Trimestralmente il DPO convocherà tutti i Responsabili del Trattamento al fine di rendere più performante le attività di trattamento. Ogni Incident di sicurezza dovrà essere reso noto all'intera struttura, per il tramite del DPO, per mezzo di comunicazioni ufficiali mirate alla minimizzazione del rischio. Dovendo il Responsabile del Trattamento dei dati coordinare l'Organizzazione interna del proprio Settore avrà l'onere di consegnare la Lettera d'incarico al trattamento dei dati personali ad ogni singolo impiegato dell'Ente facente parte della suddetta Unità Organizzativa. Tale Lettera, firmata dal Responsabile del Trattamento/Responsabile dell'Unità Organizzativa, dovrà essere firmata per accettazione dall'Incaricato, dovrà essere fotocopiata e la fotocopia sarà consegnata all'Incaricato del trattamento, mentre l'originale sarà custodito dal Responsabile dell'Unità Organizzativa /Settore. Ogni singolo dipendente afferente l'Area di riferimento dovrà ricevere tale Lettera d'Incarico. Si prega di comunicare tempestivamente al DPO ogni variazione intervenuta: trasferimenti da e verso altre Aree, nuove assunzioni, pensionamenti, altro).
La partecipazione ai corsi di formazione del personale afferente l'Unità Organizzativa sarà a cura del Responsabile del Trattamento dei dati dell'Unità Organizzativa; il quale dovrà verificare che tutti i dipendenti (persone autorizzate al trattamento) che trattano dati presso tale Area siano stati formati con l'obbligo di indicare al DPO i nominativi di chi ancora non abbia partecipato ai corsi che periodicamente vengono effettuati. In quanto, il trattamento dei dati è sub judice ad una formazione continua e nondimeno, con l'entrata in vigore del GDPR (UE 2016679), ad esporre l'intera Azienda a Verifiche da parte del Garante Privacy in funzione anche di eventuali Data Breach