

Regolamento aziendale in merito al trattamento dei dati personali ai sensi del Reg. (UE) 2016/679 “GDPR”

TITOLARE DEL TRATTAMENTO: AST Macerata

Sede: Via Domenico Annibaldi, 31 – Piediripa di Macerata (MC)

PEC: ast.macerata@emarche.it

Versione/Revisione: 2.0

Data di revisione: 12/11/2024

Sommario

INTRODUZIONE	3
Art. 1. - Definizioni	5
Art. 2. - Quadro normativo di riferimento.....	5
Art. 3. - Finalità	6
Art. 4. - Definizioni	6
CAPO II – PRINCIPI.....	8
Art. 5. - Principi e responsabilizzazione.....	9
Art. 6. - Informativa.....	9
Art. 7. - Sensibilizzazione e formazione.....	11
CAPO III – IL TRATTAMENTO DEI DATI PERSONALI	12
Art. 8. - Basi giuridiche per trattare dati personali comuni	12
Art. 9. - Basi giuridiche per trattare dati personali particolari.....	13
Art. 10. - Diritto all’anonimato	14
Art. 11. - Materie di interesse pubblico rilevante	15
Art. 12. - Altri riferimenti in ambito sanitario del Codice Privacy.....	16
Art. 13. - Condizioni per il consenso in materia di protezione dati personali	17
Art. 14. - Trattamento dei dati personali comuni e dati sensibili/particolari e giudiziari	18
Art. 15. - Trattamento dei dati del personale	19
Art. 16. - Registro delle attività di trattamento e delle categorie di trattamento	20
Art. 17. - Valutazione di impatto (DPIA).....	21
Art. 18. - Accesso ai data base e profili di autorizzazione	21
CAPO IV – DIRITTI DEGLI INTERESSATI	22
Art. 19. - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.....	22
Art. 20. - Diritto di accesso ai documenti amministrativi, diritto di accesso civico e protezione dei dati personali	23
Art. 21. - Diritti dell’interessato	23
Art. 22. - Diritto di accesso in relazione ai trattamenti dei dati personali.....	23
Art. 23. - Diritto alla rettifica e cancellazione.....	24
Art. 24. - Diritto alla limitazione	25
Art. 25. - Diritto alla portabilità.....	25
Art. 26. - Diritto di opposizione e processo decisionale automatizzato relativo alle persone.....	26
Art. 27. - Limiti all’esercizio dei diritti dell’interessato	26
Art. 28. - Modalità di esercizio dei diritti dell’interessato	27
Art. 29. - Indagini difensive	28
Art. 30. - Accesso ai dati da parte dell’Autorità Giudiziaria.....	29

CAPO V – SOGGETTI.....	29
Art. 31. - Titolare e contitolari.....	29
Art. 32. - Soggetti Autorizzati al trattamento.....	30
Art. 33. - Designati al trattamento	30
Art. 34. - Incaricati al trattamento	31
Art. 35. - Incaricati al trattamento per specifiche attività, non dipendenti del Titolare.....	32
Art. 36. - Responsabili esterni del trattamento e sub-responsabili esterni.....	32
Art. 37. - Amministratore di Sistema.....	34
Art. 38. - Responsabile della protezione dei dati personali (RPD) – Data Protection Officer (DPO).....	34
CAPO VI – SICUREZZA DEI DATI PERSONALI	35
Art. 39. - Misure di sicurezza.....	35
Art. 40. - Valutazione d’impatto sulla protezione dei dati (DPIA)	36
Art. 41. - Pubblicazione sintesi della valutazione d’impatto – DPIA.....	38
Art. 42. - Consultazione preventiva.....	38
Art. 43. - Modulistica e procedure	39
Art. 44. - Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali	
Art. 45. - Notificazione di una violazione dei dati personali.....	39
Art. 46. - Comunicazione di una violazione dei dati personali	40
Art. 47. - Disposizioni finali.....	41

INTRODUZIONE

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito anche «GDPR»), con abrogazione della direttiva 95/46/CE (Direttiva relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, d'ora in poi «Direttiva»).

Il GDPR, che si applica negli Stati membri a decorrere dal 25 maggio 2018, si fonda sulla affermazione che la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale come risulta anche dalla circostanza che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'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.

Per rafforzare la protezione dei dati personali, il Regolamento introduce numerose e rilevanti novità partendo da un approccio, fondato sul principio di cautela, basato sul rischio del trattamento e su misure di *accountability* di titolari e responsabili (come la valutazione di impatto, il registro dei trattamenti, le misure di sicurezza, la nomina di un RDP/DPO).

Come ha evidenziato il Garante per la Protezione dei Dati Personali («Garante») nella guida all'applicazione del Regolamento, la nuova disciplina europea pone con forza l'accento sulla “responsabilizzazione” (*accountability*) di titolari e responsabili ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. Tra i criteri che i titolari e i responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono:

- il criterio del “*data protection by default and by design*”, ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili “al fine di soddisfare i requisiti” del Regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati;
- il criterio del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati, impatti che devono essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

Ne consegue che l'intervento delle Autorità di Controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente *ex post*, ossia a collocarsi successivamente alle determinazioni assunte autonomamente dal Titolare; ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice in materia di protezione dei dati personali («codice privacy»), come la notifica preventiva dei

trattamenti all'Autorità di Controllo e il cosiddetto *prior checking* (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del Titolare/Responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Il diritto alla privacy è un diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato. Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori delle pubbliche amministrazioni, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.

AST Macerata, in qualità di Titolare del trattamento, intende adeguare e conformare la propria attività alle novità introdotte dal GDPR, fermo restando che il presente documento è destinato ad essere aggiornato in presenza di sopravvenienza di linee guida del Garante per protezione dei dati personali o di novità normative e giurisprudenziali.

Il presente Regolamento riveste il ruolo di "vademecum" ed è pensato in due parti distinte:

- una prima parte, dal taglio teorico, che fornisce le nozioni fondamentali della nuova disciplina europea in materia di protezione dati, tale da poter costituire una vera politica di protezione dei dati personali per il Titolare e per i dipendenti nell'ambito dei trattamenti effettuati;
- una seconda parte, dal taglio pratico, che predispone un insieme di procedure operative da porre in essere, derogabili da eventuali disposizioni emanate per specifici trattamenti (dalla legge o dall'Ente), da seguire nell'applicazione del Regolamento (UE) 2016/679 ("GDPR").

Art. 1. - Definizioni

Il presente Regolamento aziendale disciplina la tutela delle persone in ordine al trattamento dei dati personali da parte dell'Azienda Sanitaria Territoriale di Macerata (per brevità di seguito "Azienda" o "AST Macerata" o "AST"), nel rispetto di quanto previsto dal Decreto Legislativo 30.6.2003 n. 196 "Codice in materia di protezione dei dati personali", da ultimo modificato dal D.Lgs. 10.8.2018, n. 101, ed in conformità al Regolamento UE 27.4.2016, n. 2016/679 ("GDPR" o "Regolamento UE"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Art. 2. - Quadro normativo di riferimento

1. Il presente Regolamento tiene conto dei seguenti documenti:
 - Codice in materia di dati personali (D.lgs. n. 196/2003 s.m.i.);
 - Linee guida e raccomandazioni dell'Autorità Garante per la protezione dei dati personali;
 - Regolamento (UE) 2016/679 (o GDPR) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
 - D.lgs. n. 101/2018 di adeguamento della normativa interna al GDPR e successive modificazioni/integrazioni;
 - Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) – 14/EN;
 - Linee-guida sui responsabili della protezione dei dati (RPD) – WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
 - Linee-guida sul diritto alla "portabilità dei dati" – WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
 - Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento – WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
 - Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 – WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
 - Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative – WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione – WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (*data breach notification*) – WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità – 13/EN WP 203.

Art. 3. - Finalità

1. Il presente Regolamento sostituisce integralmente ogni altro precedente Regolamento interno, o comunque applicabile all'AST Macerata, in materia di protezione dei dati personali.
2. Il Titolare 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'integrità e alla disponibilità delle informazioni personali e dell'identità personale e nel rispetto dei diritti e le libertà degli interessati, a prescindere dalla loro nazionalità o della loro residenza.
3. Il Titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.
4. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del Titolare, devono essere gestiti conformemente alle disposizioni del Codice, del GDPR e del presente Regolamento.

Art. 4. - Definizioni

1. Ai fini del presente Regolamento e, comunque, in sede di trattamento di dati personali da parte dell'Azienda, s'intende per:
 - a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la 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;
 - b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- d) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- e) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- f) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- g) «**titolare del trattamento**»: la persona fisica o giuridica, l'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 i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- h) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, esterni all'organizzazione dell'Azienda, che tratta dati personali per conto del titolare del trattamento;
- i) «**designato del trattamento**»: la persona fisica che tratta dati personali per conto del titolare del trattamento alla quale è affidato il coordinamento e la vigilanza delle operazioni di trattamento dei dati personali effettuate dagli incaricati;
- j) «**autorizzato del trattamento**»: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento;
- k) «**interessato**»: la persona fisica cui si riferiscono i dati personali;
- l) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- m) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- n) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- o) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- p) «**dati genetici**»: 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;
- q) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- r) «**dati relativi alla salute**»: 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;
- s) «**dati anonimi**»: i dati che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- t) «**comunicazione**»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare o del responsabile non stabiliti nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- u) «**diffusione**»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- v) «**autorità di controllo**»: l'autorità pubblica indipendente individuata nel Garante per la protezione dei dati personali.

CAPO II – PRINCIPI

Art. 5. - Principi e responsabilizzazione

1. I principi cardine del GDPR sono integralmente recepiti nell'ordinamento interno del Titolare, per effetto dei quali i dati personali sono:
 - a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
 - b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");
 - c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base del principio di "minimizzazione dei dati";
 - d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati base del principio di "esattezza";
 - e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "limitazione della conservazione";
 - f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza";
 - g) configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo in caso di necessità ("principio di necessità").
2. Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di provarlo in base al principio di "responsabilizzazione" (o *accountability*).

Art. 6. - Informativa

1. Il Titolare, al momento della raccolta dei dati personali, fornisce all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dall'art. 13 e 14 del GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
2. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.
3. L'informativa è fornita, mediante idonei strumenti:
 - a) attraverso appositi moduli da consegnare agli interessati in cui sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti.
 - b) avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante apposita pubblicazione sulla sezione dedicata del sito web istituzionale;
 - c) apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, ed altri soggetti che entrano in rapporto con il Titolare;
 - d) resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure, anche tramite diciture brevi richiamanti informative più ampie.
4. L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
5. L'informativa contiene il seguente contenuto minimo:
 - a) l'identità e i dati di contatto del Titolare e, ove presente, del suo rappresentante;
 - b) i dati di contatto del RPD/DPO ove esistente;
 - c) le finalità del trattamento;
 - d) i destinatari dei dati;
 - e) la base giuridica del trattamento;
 - f) l'interesse legittimo del Titolare se quest'ultimo costituisce la base giuridica del trattamento;
 - g) se il Titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
 - h) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;

- i) il diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
 - j) il diritto di presentare un reclamo all'autorità di controllo;
 - k) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.
6. Nel caso di dati personali non raccolti direttamente presso l'interessato:
- a) il Titolare deve informare l'interessato anche in merito a:
 - i. le categorie di dati personali trattati;
 - ii. la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;
 - b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.
7. Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del Titolare è predisposta apposita informativa per personale dipendente.
8. Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.
9. Nel fornire l'informativa, il Titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati particolari e giudiziari. È prevista la possibilità di fornire informative "brevi" che richiamino informative più estese.

Art. 7. - Sensibilizzazione e formazione

- 1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, AST Macerata si impegna a sostenere e a promuovere a tutti i livelli, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della protezione dei dati e migliorare la qualità del servizio.
- 2. A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale del Titolare e l'attività informativa diretta a tutti coloro che hanno rapporti con il Titolare.

3. Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è fornita a ogni dipendente una specifica comunicazione in merito alla necessità di allinearsi alle presenti disposizioni in materia di protezione dei dati, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito del Titolare.
4. Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.
5. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, anche eventualmente integrati con gli interventi di formazione anticorruzione, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.
6. La formazione in materia di prevenzione dei rischi di violazione dei dati personali può essere integrata e coordinata anche con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il Titolare.
7. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione dell'*accountability* dell'Ente.

CAPO III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 8. - Basi giuridiche per trattare dati personali comuni

1. Il GDPR, all'art. 6, disciplina il trattamento di dati personali **comuni** definendo le condizioni di liceità tra una delle seguenti condizioni:
 - a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
 - b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
 - c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
 - d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
 - e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

- f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
2. Ad un ente pubblico nell'esecuzione dei propri compiti non si applica la lettera f) del precedente comma, pertanto l'azienda sanitaria nelle attività di prevenzione, diagnosi, cura, riabilitazione o ricerca scientifica non utilizza la base giuridica del legittimo interesse del Titolare.

Art. 9. - Basi giuridiche per trattare dati personali particolari

1. Il GDPR, all'art. 9, disciplina il trattamento di categorie **particolari** di dati personali. Nello specifico il Regolamento sancisce il divieto di trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Dopodiché afferma che tale divieto non si applica laddove:
- a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
 - b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
 - c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
 - d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
 - e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
 - f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

- 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;
 - 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;
 - i) 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;
 - j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
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.

Art. 10. - Diritto all'anonimato

1. L'Azienda garantisce, nell'ambito dei dati previsti dall'art. 9 del Regolamento UE, l'adempimento dell'obbligo di un trattamento dei dati non immediatamente identificativi del cittadino-utente, che si realizza, di norma, attraverso l'utilizzo di codici alfanumerici o di altre forme di pseudonimizzazione.
2. Il trattamento dei dati relativi alle seguenti informazioni è sottoposto ad un regime normativo di particolare tutela:
 - sieropositività;
 - interruzione volontaria di gravidanza;
 - vittime di violenza sessuale o di pedofilia;

- uso di sostanze stupefacenti, di sostanze psicotrope e di alcool;
- parto in anonimato.

Art. 11. - Materie di interesse pubblico rilevante

1. In riferimento alla lettera g) dell'art. 9 GDPR, il D.lgs. 101/2018, modificando il Codice Privacy, inserendo l'art. 2-sexies, ha individuato un'elencazione di materie rientranti nell'ambito dell'interesse pubblico rilevante, molto importante per le Pubbliche Amministrazioni.
2. Tale articolo prevede che:
 - a) I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
 - b) Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:
 - i. accesso a documenti amministrativi e accesso civico;
 - ii. attività di controllo e ispettive;
 - iii. concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
 - iv. conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
 - v. rapporti tra i soggetti pubblici e gli enti del terzo settore;
 - vi. obiezione di coscienza;
 - vii. rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
 - viii. attività socioassistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

- ix. attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;
- x. compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- xi. programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
- xii. vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
- xiii. tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
- xiv. istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- xv. trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
- xvi. instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

Art. 12. - Altri riferimenti in ambito sanitario del Codice Privacy

1. In attuazione di quanto previsto dall'articolo 9 GDPR e dell'art. 2-septies del Codice, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di liceità previste ed in conformità alle misure di garanzia disposte dal Garante, con apposito provvedimento.
2. Ai sensi dell'art. 2-terdecies del Codice Privacy, i diritti di cui agli articoli da 15 a 22 GDPR, riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce

a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione, tenendo conto di eventuali divieti dell'interessato.

3. Ai sensi dell'art. 110 del Codice, per quanto concerne la Ricerca medica, biomedica ed epidemiologica, il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del Codice.
4. Si rimanda al Titolo V (artt. 75 ess.) del Codice per gli ulteriori approfondimenti in tema di trattamento di dati personali in ambito sanitario.

Art. 13. - Condizioni per il consenso in materia di protezione dati personali

1. Il trattamento di dati personali nell'ambito delle finalità di prevenzione, diagnosi, assistenza, riabilitazione e cura non necessitano di acquisizione del consenso ma sono basati sulle basi giuridiche indicate negli articoli precedenti
2. Il consenso al trattamento dei dati personali è invece previsto nelle ipotesi di:
 - a) Costituzione del Dossier Sanitario Elettronico (DSE/DSOE);
 - b) Consultazione dei Referti On-Line;
 - c) Ricerca scientifica;
 - d) Comunicazioni dello stato di salute al medico curante, a familiari e conoscenti.
3. Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

4. Per i dati sensibili/particolari il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione.
5. Se il consenso dell'interessato al trattamento dei propri dati personali è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione, che costituisca una violazione del GDPR e del presente Regolamento, è vincolante.
6. In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.
7. Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, predisposta dal Titolare, previa consegna e presa d'atto dell'informativa.
8. Non è ammesso il consenso tacito o presunto ovvero l'utilizzo di caselle pre-spuntate su un modulo.
9. Il Titolare adotta misure organizzative adeguate a facilitare l'espressione del consenso da parte dell'interessato.
10. La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso alle prestazioni, ed è valido ed efficace fino alla revoca della stessa o, per i minorenni, fino al compimento del diciottesimo anno di età.
11. Il consenso viene registrato nel registro delle attività di trattamento.

Art. 14. - Trattamento dei dati personali comuni, dei dati particolari e giudiziari

1. Il Titolare conforma il trattamento dei dati sensibili/particolari e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. A tale fine, il Titolare si conforma ai principi del GDPR e del Codice per la protezione dei dati e si conforma alle Linee Guida del Garante in materia. Laddove possibile i dati idonei a rivelare lo stato di salute e la vita

sessuale sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

3. Il Titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili/particolari e giudiziari.

Art. 15. - Trattamento dei dati del personale

1. Il Titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità di instaurazione e di gestione di rapporti di lavoro di qualunque tipo, nel rispetto degli obblighi di legge e per assolvere gli obblighi o esercitare diritti specifici del titolare o dell'interessato in materia di diritto del lavoro.
2. Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
3. Secondo la normativa vigente, il Titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere e l'origine razziale ed etnica.
4. Il trattamento dei dati sensibili/particolari del dipendente, da parte del datore di lavoro, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo dei dati giudiziari e sensibili/particolari, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.
5. La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici. Non sono infatti ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.
6. Il Titolare, nel trattamento dei dati sensibili/particolari relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.

7. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 16. - Registro delle attività di trattamento e delle categorie di trattamento

1. Il Titolare del trattamento istituisce un registro, in forma digitale, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità.
2. Il registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo. In ossequio all'art. 30 GDPR, tale registro contiene le seguenti informazioni:
 - a) il nome e i dati di contatto del Titolare del trattamento, del Responsabile per la protezione dei dati, dei responsabili e degli incaricati;
 - b) le finalità del trattamento;
 - c) una descrizione delle categorie di interessati e delle categorie dei dati personali;
 - d) le categorie dei trattamenti effettuati;
 - e) le categorie di destinatari, a cui i dati personali sono o saranno comunicati;
 - f) l'indicazione delle cautele specifiche, a cui ciascun Responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
 - g) un'eventuale possibilità di trasferimenti di dati all'estero;
 - h) una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;
 - i) indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.
3. Laddove l'Ente svolga il ruolo di responsabile esterno, tiene il registro dei trattamenti del Responsabile contenente:
 - a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del Titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
 - b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
 - c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al paragrafo 2 dell'articolo 49, la documentazione delle garanzie adeguate;
 - d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR.

4. Su richiesta, il Titolare del trattamento o il responsabile del trattamento, mettono il registro a disposizione del Garante.

Art. 17. - Valutazione di impatto (DPIA)

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati (DPO/RPD).
3. La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:
 - a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
 - b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
 - c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

Art. 18. - Accesso ai data base e profili di autorizzazione

1. Nel rispetto del principio di necessità e pertinenza del trattamento dei dati personali, i profili di accesso ai gestionali informatici aziendali sono configurati sulla base delle attività affidate a ciascun autorizzato e nel rispetto degli ambiti di trattamento consentiti. L'assegnazione dei predetti profili ai singoli operatori incaricati del trattamento dei dati è effettuata a cura dei rispettivi responsabili Designati.
2. Per ciascuna banca dati (applicativo informatico) deve essere definito l'elenco dei profili di accesso e le loro specificità mediante la previsione di profili diversi di abilitazione in funzione della diversa tipologia di operazioni consentite.
3. In ogni caso gli accessi ai dati personali contenuti nei data base aziendali, nel rispetto del principio di minimizzazione, devono essere ridotti allo stretto necessario per consentire l'espletamento delle ordinarie attività lavorative.

4. Il trattamento dei dati deve, pertanto, essere evitato ogni volta in cui lo stesso non sia indispensabile per il perseguimento degli scopi prefissati.
5. Periodicamente i Designati aggiornano i profili di autorizzazione del personale assegnato.
6. Al fine di garantire che il trattamento dei dati inerenti allo stato di salute degli interessati sia effettuato con un idoneo livello di sicurezza, gli accessi ai software contenenti dati particolari devono essere tracciati.

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 19. - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. Il Titolare, in sede di pubblicazione e diffusione, anche tramite l'albo pretorio informatico, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:
 - a) sicurezza
 - b) completezza
 - c) esattezza
 - d) accessibilità
 - e) minimizzazione
 - f) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.
2. Laddove documenti, dati e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati o pseudonimizzati, tranne deroghe previste da specifiche disposizioni.
3. Salva diversa disposizione di legge, il Titolare garantisce la riservatezza dei dati sensibili/particolari in sede di pubblicazione tramite Albo pretorio online, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il Titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.
4. Il Titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Art. 20. - Diritto di accesso ai documenti amministrativi, diritto di accesso civico e protezione dei dati personali

1. I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato, contenenti dati personali, e la relativa tutela giurisdizionale nonché le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati sensibili/particolari e giudiziari.
2. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
3. Il Titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 21. - Diritti dell'interessato

1. Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel GDPR e nel Codice.
2. La procedura e il modulo per esercitare i diritti in materia di protezione dei sono pubblicati sul sito istituzionale, nell'apposita sezione, assieme alle informative in materia di trattamento dei dati personali.

Art. 22. - Diritto di accesso in relazione ai trattamenti dei dati personali

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale 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 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. 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.
 3. 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 l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
 4. Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 23. - Diritto alla rettifica e cancellazione

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione («diritto all'oblio»), di seguito indicata.
2. Quanto al diritto di rettifica, 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.
3. Il Titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
4. Quanto al diritto "all'oblio", consistente nel diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:
 - a) per l'esercizio del diritto alla libertà di espressione e di informazione;
 - b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
 - c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 GDPR;

- d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 24. - Diritto alla limitazione

1. Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto alla limitazione, di seguito indicata. L'interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:
 - a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza di tali dati personali;
 - b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
 - c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
 - d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 GDPR, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal Titolare prima che detta limitazione sia revocata.
4. Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 25. - Diritto alla portabilità

1. Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del GDPR, il diritto alla portabilità dei dati non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Art. 26. - Diritto di opposizione e processo decisionale automatizzato relativo alle persone

1. 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) GDPR, compresa la profilazione sulla base di tali disposizioni.
2. 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. Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
3. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Art. 27. - Limiti all'esercizio dei diritti dell'interessato

1. Sia il GDPR sia il D.lgs. n. 196/2003, così come modificato dal D.lgs. n. 101/2018, prevedono delle ipotesi in cui è possibile limitare l'esercizio dei diritti dell'interessato. Nello specifico l'art. 23 GDPR prevede che il diritto dello Stato membro cui è soggetto il Titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:
 - a) la sicurezza nazionale;
 - b) la difesa;
 - c) la sicurezza pubblica;

- d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
 - e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
 - f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
 - g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
 - h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
 - i) la tutela dell'interessato o dei diritti e delle libertà altrui;
 - j) l'esecuzione delle azioni civili.
2. L'art. 2-undecies del Codice Privacy, di conseguenza, prevede che i diritti di cui agli articoli da 15 a 22 del GDPR non possono essere esercitati con richiesta al Titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:
- a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
 - b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
 - c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
 - d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
 - e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
 - f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

Art. 28. - Modalità di esercizio dei diritti dell'interessato

1. Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice, del presente Regolamento e della relativa procedura, di seguito descritta.
2. La richiesta per l'esercizio dei diritti può essere fatta pervenire:

- a) direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso, come ad esempio, la conoscenza personale;
 - b) tramite chi esercita la potestà o la tutela, per i minori e gli incapaci;
 - c) in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
 - d) dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.
3. L'interessato può presentare o inviare la richiesta di esercizio dei diritti utilizzando l'apposita modulistica pubblicata sul sito web aziendale:
- a) al Titolare o Referente del trattamento, che conserva e gestisce i dati personali dell'interessato;
 - b) all'ufficio protocollo generale del Titolare o all'ufficio per le relazioni con il pubblico;
 - c) all'indirizzo e-mail del DPO/RPD.
4. La richiesta per l'esercizio dei diritti di accesso ai dati personali può essere esercitata dall'interessato solo in riferimento alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.
5. Fermo restando l'accesso ai dati personali, il Dirigente autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.
6. I soggetti competenti alla valutazione dell'istanza sono il Titolare e il Responsabile per la protezione dei dati (DPO) che decidono sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati.
7. All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo. L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del Titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.
8. Il Titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 29. - Indagini difensive

1. Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del Titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.

2. Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'interessato, e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento del Titolare sul diritto di accesso.
3. Il Titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

Art. 30. - Accesso ai dati da parte dell'Autorità Giudiziaria

1. Il personale in forza all'Autorità Giudiziaria (pubblico ministero e polizia giudiziaria) accedono e richiedono copia dei dati personali in possesso dell'organizzazione esclusivamente dietro presentazione di richiesta da parte del Pubblico Ministero ove sia indicato il numero di iscrizione al Registro delle Notizie di Reato (R.G.N.R.) o dietro specifica richiesta in cui emerge il presupposto giuridico (denuncia, esposto, querela) di coloro che nello svolgimento dell'attività di Polizia Giudiziaria svolgono attività di iniziativa.

CAPO V – SOGGETTI

Art. 31. - Titolare e contitolari

1. Il Titolare del trattamento è AST Macerata, rappresentato dal Direttore Generale, in qualità di legale rappresentante con sede Via Domenico Annibaldi, 31 – Piediripa di Macerata (MC).
2. Il Titolare provvede:
 - a) a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al Codice, al GDPR e al presente Regolamento;
 - b) a nominare, con proprio atto, il Responsabile per la protezione dei dati personali (RPD/DPO);
 - c) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
 - d) a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
 - e) ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.
3. Il Titolare si trova in rapporto di contitolarità con altri titolari quando determinano congiuntamente le finalità e i mezzi del trattamento.
4. I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e 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 GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei titolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

5. Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun Titolare del trattamento.

Art. 32. - Soggetti Autorizzati al trattamento

1. Il GDPR non prevede particolari formalità per l'individuazione dei soggetti che trattano i dati all'interno di un'organizzazione, ma richiede (in ossequio al principio dell'*accountability*) una tracciabilità delle autorizzazioni al trattamento. In tal senso il GDPR fa riferimento in più punti al *“personale che ha accesso permanente o regolare ai dati personali”*, o a *“le persone autorizzate al trattamento dei dati personali”*.
2. Il nuovo Codice, abbandonando il concetto di “Lettera di Incarico”, prevede più semplicemente che sia il Titolare a individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che effettuano operazioni di trattamento sotto la propria autorità (art. 2-quaterdecies Codice Privacy).
3. A tal fine, con il presente Regolamento, si individuano diversi livelli di autorizzazione funzionale, coerentemente con l'organigramma dell'Ente e, in linea generale, si prevede che le autorizzazioni, ex 2-quaterdecies Codice privacy e ex art. 29 GDPR, a trattare i dati personali sono connesse alle autorizzazioni relative ai profili informatici assegnati ai vari dipendenti.
4. Si specifica che, sotto il profilo del trattamento dei dati personali, i soggetti autorizzati si suddividono in:
 - a) Designati.
 - b) Incaricati.

Art. 33. - Designati al trattamento

1. Con il presente Regolamento si individuano i Designati al trattamento, ossia i soggetti mediante i quali AST Macerata esercita le proprie funzioni di Titolare del trattamento. In forza del presente Regolamento, infatti, sono nominati quali designati al trattamento dei dati:
 - a) Direttore Amministrativo, Direttore Sanitario e Direttore Socio-sanitario,
 - b) Direttore medico di Presidio Ospedaliero, Direttori di Dipartimento, Direttori di Distretto sanitario, Direttori professioni tecnico – sanitarie,

in ragione e nei limiti del loro mandato;

c) Dirigenti di UOC/UOSD/UOS, nell'ambito dei trattamenti effettuati nella relativa Unità Operativa.

2. Queste figure sono i riferimenti del Titolare, il quale, con il presente Regolamento, impartisce a essi le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati e all'eventuale uso di apparecchiature di videosorveglianza.
3. Con il presente Regolamento (**Allegato 1.1**) gli stessi sono informati delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice Privacy e dal GDPR.
4. Nell'attuazione dei compiti loro indicati, i soggetti sopra individuati, qualora la legge lo imponga o essi lo ritengano necessario, contattano senza indugio il DPO e, se necessario, acquisiscono il suo parere.
5. Ciascun Designato risponde al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e dal presente Regolamento, oltreché della mancata attuazione delle misure di sicurezza.
6. Al momento del conferimento dell'incarico/sottoscrizione del contratto/nomina sono fornite, a cura della U.O.C. Gestione Risorse Umane, ad ogni designato, oltre apposita informativa ex art. 13 GDPR, opportune "istruzioni operative" (**Allegato 1.1 e Allegato 1.3 per il personale sanitario**).

Art. 34. - Incaricati al trattamento

1. Con il presente Regolamento si stabilisce che il personale dipendente del Titolare, che operano sotto la diretta autorità del Titolare, con il presente Regolamento sono autorizzati, in relazione ai compiti loro conferiti, al trattamento dei dati personali nel rispetto delle mansioni ricoperte e nei limiti delle finalità connesse al rapporto di lavoro con l'Azienda, coerentemente con quanto previsto dalle norme vigenti e dal presente Regolamento.
2. Ogni soggetto dipendente del Titolare, preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è individuato e nominato quale autorizzato ai sensi dell'art. 2-*quaterdecies* del Codice nonché ai sensi degli artt. 4 par. 10 e art. 29 del GDPR.
3. Tali soggetti sono formalmente autorizzati tramite assegnazione funzionale della persona fisica alla unità organizzativa.
4. Gli incaricati collaborano con il Titolare e il Designato segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
5. Con il presente Regolamento (Errore. L'origine riferimento non è stata trovata. si impartiscono a essi le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e

diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza. Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e dal Designato, nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del Titolare.

6. Al momento dell'ingresso in servizio sono fornite, a cura della U.O.C. Gestione Risorse Umane, ad ogni dipendente, oltre apposita informativa ex art. 13 GDPR, le opportune "istruzioni operative" (**Allegato 1. 2 e Allegato 1. 3 per il personale sanitario**).

Art. 35. - Incaricati al trattamento per specifiche attività, non dipendenti del Titolare

1. Tutti i soggetti che svolgono un'attività di trattamento dei dati e che non sono dipendenti del Titolare o che operano temporaneamente all'interno della struttura organizzativa del Titolare o che svolgono solo specifici e limitati interventi sui dati personali (a titolo meramente esemplificativo, il personale medico convenzionato, i tirocinanti, i titolari di contratti di collaborazione coordinata e continuativa e di contratti libero professionali e/o altri soggetti, eventualmente anche individuati dai designati) devono essere autorizzati nominativamente al trattamento tramite apposito atto scritto di nomina. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare.
2. Questi ultimi sono soggetti agli stessi obblighi a cui sono sottoposti tutti gli incaricati del Titolare, salvo specifiche istruzioni afferenti al servizio svolto, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
3. Gli incaricati non dipendenti dal Titolare, valutato caso per caso, possono essere destinatari degli interventi di formazione di aggiornamento.
4. Ai soggetti di cui al paragrafo 1) la U.O.C. competente all'attivazione di specifici contratti consegnerà, oltre apposita informativa ex art. 13 GDPR, le opportune "istruzioni operative" (**Allegato 1. 2 e Allegato 1. 3 per il personale sanitario**).

Art. 36. - Responsabili esterni del trattamento e sub-responsabili esterni

1. Il Responsabile esterno è il soggetto che, in ragione di un rapporto giuridico, agisce per conto del Titolare.
2. Il Responsabile è designato dal Titolare. I Responsabili esterni vengono nominati dal Titolare del trattamento e/o, per esso, dai soggetti individuati quali Designati del Titolare. Circa le modalità della predetta nomina, ciascun Designato utilizzerà apposita modulistica allegata (**Allegato 1. 4**). L'utilizzo di

moduli diversi da quello approvato ed allegato al presente Regolamento dovranno essere sottoposti al DPO aziendale per una sua valutazione di ammissibilità.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il Titolare può avvalersi, per il trattamento di dati, anche sensibili/particolari, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se nominato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
4. Il Responsabile del trattamento non ricorre a un altro Responsabile (sub-responsabile) senza previa autorizzazione scritta, specifica o generale, del Titolare o, per esso, dai soggetti Designati.
5. Il Titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, può designare quali Responsabili del trattamento dei dati personali, unicamente i soggetti 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 (art. 28 del GDPR).
6. I Responsabili e i sub-responsabili del trattamento hanno l'obbligo di:
 - a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;
 - b) rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
 - c) nominare al loro interno i soggetti autorizzati al trattamento o individuarli tramite altri criteri espressi;
 - d) garantire che i dati trattati siano portati a conoscenza soltanto del personale autorizzato al trattamento;
 - e) trattare i dati personali, anche di natura sensibile e sanitaria, dei Pazienti esclusivamente per le finalità previste dal contratto o dalla convenzione;
 - f) attenersi alle disposizioni impartite dal Titolare del trattamento;
 - g) specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
 - h) comunicare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
7. Nel caso di mancato rispetto delle già menzionate disposizioni, e in caso di mancata comunicazione al Titolare dell'atto di nomina dei soggetti autorizzati al trattamento dei dati, laddove richiesti, ne risponde

direttamente, verso il Titolare, il Responsabile del trattamento. La nomina del Responsabile viene effettuata mediante atto da parte del Titolare del trattamento o dal Designato, da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente al Titolare.

8. L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 37. - Amministratore di Sistema

1. L'amministratore di sistema, individuato nel Dirigente Responsabile del Centro Elaborazione Dati, sovrintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.
2. L'amministratore di sistema svolge attività, quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.
3. Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (*access log*) devono essere complete, inalterabili, verificabili nella loro integrità, e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
4. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.
5. Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
6. Il Titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
7. L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Art. 38. - Responsabile della protezione dei dati personali (RPD) – Data Protection Officer (DPO)

1. Il Titolare designa il Responsabile della protezione dei dati (RPD/DPO).
2. Il RPD/DPO deve essere in possesso di:
 - a) un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;

- b) deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- c) operare alle dipendenze del Titolare del trattamento oppure sulla base di un contratto di servizio.

Il RPD/DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

3. Il Titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.
4. Il RPD/DPO svolge i seguenti compiti:
 - a) informa e fornisce consulenze al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
 - b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
 - c) fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
 - d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
 - e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

CAPO VI – SICUREZZA DEI DATI PERSONALI

Art. 39. - Misure di sicurezza

1. Il Titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
2. In particolare, il Titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate a garantire un livello di sicurezza adeguato al rischio. Tali misure che comprendono almeno:
 - a) la pseudonimizzazione e la cifratura dei dati personali trattati;
 - b) procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - c) modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;

- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- 3. Per quanto attiene al trattamento dei dati personali effettuato con strumenti elettronici e non, il Titolare applica le misure di sicurezza che si reputano adeguate alle diverse circostanze e al proprio contesto.

Art. 40. - Valutazione d'impatto sulla protezione dei dati (DPIA)

1. La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
2. La DPIA è uno strumento importante per la responsabilizzazione in quanto sostiene il Titolare non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.
3. La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal Titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, intendendosi per "rischio" uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, e per "gestione dei rischi" l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
4. Prioritariamente alla DPIA deve:
 - a) essere effettuata o aggiornata la ricognizione dei trattamenti;
 - b) essere effettuata la determinazione in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati.
5. La decisione in ordine alla possibilità che il trattamento possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA viene adottata applicando i casi indicati l'art. 35, paragrafo 3 del GDPR e i criteri esplicativi contenuti nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida").
6. Nell'applicare i suddetti criteri si deve tenere conto di quanto segue:
 - a) la DPIA è sempre obbligatoria, indipendentemente dalla presenza di uno o più criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dall'Autorità di controllo ai sensi dell'art. 35, paragrafo 4 GDPR;

- b) la DPIA è sempre obbligatoria per i trattamenti inclusi nell'indice dei trattamenti dei dati sensibili/particolari e giudiziari ai sensi del Regolamento sul trattamento dei dati sensibili e giudiziari approvato dall'Ente conformemente allo schema tipo del Garante;
- c) secondo le Linee guida, un trattamento che soddisfa n. 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati; tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio costituisce elemento sufficiente per originare l'obbligo di svolgimento della DPIA;
- d) maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;
- e) se, pur applicando i criteri sopra indicati, la necessità di una DPIA non emerge con chiarezza, va comunque ritenuto sussistente l'obbligo – secondo quanto raccomandato dal WP29 – di farvi ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento.

7. La DPIA non è richiesta nei seguenti casi:

- a) quando, sulla base di predetti criteri, risulta che il trattamento non è tale da “presentare un rischio elevato per i diritti e le libertà delle persone fisiche”;
- b) quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;
- c) quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- d) qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) GDPR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GDPR).

8. La DPIA deve contenere almeno:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati;
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente

regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

9. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.
10. Per conseguire l'obiettivo della riduzione del rischio, la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme UNI ISO (31000 e 27001) nonché degli orientamenti contenuti nelle Linee guida, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del GDPR:
 - a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
 - b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
 - c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1, art. 35 del GDPR;
 - d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
11. Il Titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati (DPO).
12. Laddove la DPIA riveli la presenza di rischi residui elevati, il Titolare è tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento ai sensi dell'art. 36, paragrafo 1 GDPR.

Art. 41. - Pubblicazione sintesi della valutazione d'impatto – DPIA

1. Il Titolare, se lo ritiene opportuno, può effettuare la pubblicazione della DPIA o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal Titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.
2. La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il Titolare o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 42. - Consultazione preventiva

1. Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del RPD/DPO, il Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate.

Art. 43. - Modulistica e procedure

1. Il Titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante adotta e costantemente aggiorna:
 - a) modelli uniformi di informativa;
 - b) modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza.
2. Le versioni aggiornate della modulistica e delle procedure sono pubblicate nella sul sito web: <https://www.asur.marche.it/privacyast3>.

Art. 44. - Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

1. Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato con le sanzioni previste dagli articoli da 166 a 172 del Codice da parte del Garante, nonché con sanzioni di natura disciplinare.
2. Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.
3. Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice, nel GDPR e nel presente regolamento, e a lui specificamente diretti o qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare del trattamento.
4. Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 45. - Notificazione di una violazione dei dati personali

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno

che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. **I soggetti Designati e Incaricati informano il Titolare del trattamento senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione. La violazione dell'obbligo di informazione predetto è valutabile ai fini di una eventuale responsabilità disciplinare e/o erariale.
3. La notifica deve almeno:
 - a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
 - c) descrivere le probabili conseguenze della violazione dei dati personali;
 - d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Art. 46. - Comunicazione di una violazione dei dati personali

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR.
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
 - a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
 - b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

- c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
- 4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Art. 47. - Disposizioni finali

- 1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, le Linee guida e i provvedimenti del Garante.
- 2. Il presente Regolamento è aggiornato costantemente a seguito di ulteriori modificazioni alla vigente normativa in materia di protezione dei dati personali.

Allegato 1.1 – Istruzioni specifiche per i singoli Designati

I soggetti designati al trattamento dei dati personali compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza, disponibilità e integrità dei dati; in particolare hanno il dovere di osservare e fare osservare le precauzioni e le misure tecniche ed organizzative di protezione individuate dal Titolare.

I soggetti Designati sono tenuti:

- a supportare il Titolare nell'analisi di tutte le questioni rilevanti ai fini della normativa in materia di protezione dei dati personali;
- a comunicare al Titolare e al DPO aziendale i trattamenti in essere all'interno del proprio settore di competenza e l'eventuale inizio, modifica e/o cessazione di ogni trattamento ai fini della compilazione e del continuo aggiornamento del registro dei trattamenti.

In caso di assenza a qualsiasi titolo del soggetto Designato, la funzione di responsabilità nel trattamento dei dati personali è assunta per tutta la durata dell'assenza dal sostituto o facente funzioni senza necessità di incarico formale.

La designazione non è delegabile.

I soggetti Designati, negli ambiti di propria competenza, devono garantire il pieno rispetto del GDPR e del Codice Privacy vigente, delle linee guida dell'Autorità Garante per la protezione dei dati e dei regolamenti e delle procedure interne in materia.

Essi debbono altresì mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi su di loro ricadenti e informarlo immediatamente qualora ritengano che un'istruzione violi le disposizioni in materia di protezione dei dati.

In particolare, i soggetti Designati, nel trattamento dei dati personali, sono vincolati dal segreto professionale e hanno l'obbligo di:

- consegnare agli interessati l'informativa privacy più idonea, ex artt- 13 e 14, tra quelle predisposte dal Titolare del trattamento;
- definire l'ambito e le modalità di trattamento consentite a ciascuno degli operatori ad essi assegnati quale personale incaricato del trattamento e impartire loro istruzioni circa le misure di sicurezza da porre in essere nelle operazioni di trattamento ad essi affidate;
- provvedere a che l'interessato possa esercitare i diritti previsti dagli artt. 15 e ss del GDPR;
- verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza ed indispensabilità in rapporto agli adempimenti, provvedendo alla cancellazione degli archivi contenenti dati obsoleti e di eventuali archivi non autorizzati secondo quanto previsto dal massimario di scarto e conservazione;

- segnalare tempestivamente le eventuali situazioni di criticità nel trattamento in sicurezza dei dati personali, anche se indipendenti dalla propria potestà organizzativa;
- monitorare i rischi in materia di protezione dei dati personali relativi al settore di competenza, comunicando eventuali eventi potenzialmente dannosi per gli interessati;
- verificare periodicamente la correttezza e l'aggiornamento delle informative nel rispetto degli artt. 13-14 del GDPR, nonché il corretto trattamento dei dati personali nella propria area di competenza;
- individuare e nominare, qualora opportuno, quali incaricati color che, pur non essendo dipendenti di AST Macerata, trattano dati di cui la medesima Azienda è titolare del trattamento;
- individuare e nominare i responsabili esterni e i soggetti incaricati a compiere operazioni di trattamento, fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali aziendali;
- collaborare con il Titolare e con il DPO al fine di comunicare tempestivamente l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto;
- collaborare con il Titolare e con il DPO ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio;
- informare il Titolare e il DPO, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali e collaborare nella notificazione di una violazione dei dati personali al Garante privacy o nella comunicazione di una violazione dei dati personali all'interessato;
- se necessario, collaborare nella redazione della valutazione d'impatto sulla protezione dei dati o nell'eventuale consultazione preventiva;
- segnalare tempestivamente al DPO l'eventuale necessità, per lo svolgimento delle proprie funzioni, di nuove tipologie di trattamento rispetto a quelle già poste in essere al fine di procedere alla nuova verifica;
- se di competenza, provvedere alla gestione delle autorizzazioni necessarie all'utilizzo dei sistemi e dei servizi IT dell'azienda;
- collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- garantire al DPO i necessari permessi di accesso ai dati e ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza.

Allegato 1. 2 – Istruzioni specifiche per i singoli Incaricati

Gli incaricati devono eseguire i trattamenti secondo le disposizioni date dal Titolare e/o dal Designato della cui area/U.O. fanno parte, nel rispetto delle istruzioni adottate nel presente Regolamento.

Gli incaricati del trattamento dei dati personali sono vincolati dal segreto professionale e devono eseguire i trattamenti secondo le disposizioni ricevute. L'autorizzazione è connessa alle operazioni di elaborazione di dati personali ai quali gli incaricati hanno accesso, nell'espletamento della propria funzione e in ossequio al loro rapporto di lavoro con il Titolare del Trattamento, oltre che a quanto prescritto nel Regolamento aziendale privacy e nelle procedure aziendali.

L'autorizzazione quale incaricato al trattamento dei dati personali, pertanto, è strettamente funzionale e connessa al ruolo assegnato per contratto e non può costituire conferimento di nuova mansione o ruolo. Gli autorizzati si impegnano ad adottare tutte le misure tecniche e organizzative individuate dal Titolare.

In particolare, devono:

- trattare i dati personali solo nell'ambito delle funzioni ricoperte e dell'attività regolarmente assegnatagli;
- rispettare i principi di liceità, correttezza e trasparenza nei confronti dell'interessato;
- rispettare la riservatezza, l'integrità e la disponibilità dei dati personali che la segretezza del ruolo ricoperto richiede;
- raccogliere e registrare dati personali solo per scopi determinati, espliciti e legittimi;
- conservare i dati raccolti in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali i dati sono trattati;
- garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale;
- conformarsi alle procedure previste dal GDPR, dal Codice Privacy e dal presente regolamento in materia di protezione dei dati personali;
- fornire, se necessario, l'informativa adeguata e raccogliere e gestire gli eventuali consensi;
- custodire i dati sensibili/particolari in armadi o cassetti chiusi a chiave. Tali documenti non devono in alcun caso essere lasciati incustoditi (policy scrivania pulita);
- comunicare al soggetto Designato di riferimento l'eventuale richiesta di accesso ai dati di soggetti esterni che dimostrino di averne titolo. La eventuale comunicazione di dati personali a terzi estranei è subordinata alla presentazione di una richiesta scritta che dia conto della legittimazione del richiedente, per legge o contratto, all'accesso ai dati. Tale comunicazione dovrà, peraltro, essere

fornita formalmente per iscritto e sarà subordinata alla verifica del diritto del terzo all'accesso dei dati;

- inoltrare al Titolare e al DPO eventuali richieste di accesso, per esigenze individuali, ai propri dati personali da parte di soggetti interni o esterni all'Azienda;
- informare il Titolare e il DPO, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali e collaborare nella notificazione di una violazione dei dati personali al Garante privacy o nella comunicazione di una violazione dei dati personali all'interessato;
- per l'accesso ad archivi contenenti dati personali, specialmente se sensibili/particolari, utilizzare esclusivamente le postazioni computer assegnate. In assenza dell'incaricato il computer **non** deve essere lasciato acceso. In ogni caso il monitor deve essere posizionato in modo tale da impedire ad estranei la visuale dello schermo. Per l'utilizzo deve essere attivata la procedura di creazione dell'account di accesso. La password dovrà rimanere segreta;
- i supporti rimovibili relativi ad archivi di dati personali devono essere custoditi in armadi, protetti da cassette chiuse a chiave, e non dovranno essere lasciati inseriti nel computer o a disposizione sulle scrivanie in assenza degli incaricati. I supporti rimovibili contenenti dati personali sensibili/particolari, se non utilizzati, sono distrutti o resi inutilizzabili;
- qualora si rendano necessari interventi di manutenzione o riparazione su computer è d'obbligo concordare preventivamente modalità operative e misure di sicurezza adeguate al caso concreto;
- le postazioni computer non possono essere utilizzate per scopi personali, né dovranno ospitare procedure o programmi che non siano stati forniti dalla competente struttura aziendale o installati previa precisa autorizzazione;
- la trasmissione, tra gli Uffici interni, di documenti facenti riferimento e/o contenenti dati personali di qualunque natura va sempre effettuata con lettera di accompagnamento regolarmente protocollata. La trasmissione deve essere motivata da effettive esigenze lavorative;
- al di fuori dei casi indicati è assolutamente vietato comunicare o diffondere dati personali a terzi.

In tutti i casi in cui le operazioni di trattamento dei dati personali siano fonte di dubbio per gli incaricati o si ritenga vi sia una violazione, anche potenziale, di dati personali, gli stessi sono tenuti a rivolgersi al Responsabile per la protezione dei dati (**DPO**) per i necessari chiarimenti.

Allegato 1. 3 - Istruzioni specifiche per il personale sanitario destinate sia ai “Designati” che agli “Incaricati” al trattamento dei dati personali

PREMESSA

Le presenti istruzioni – specifiche per il personale sanitario che svolge la propria attività lavorativa in contesti, quali, l’ambito ospedaliero, ambulatori, distretti, strutture territoriali, ecc. - hanno lo scopo di chiarire e diffondere regole/misure comportamentali, organizzative e tecniche cui i professionisti “Designati” e gli “Incaricati” al trattamento devono attenersi nello svolgimento delle operazioni di trattamento dei dati personali all’interno dell’organizzazione aziendale, al fine di ridurre e contenere i rischi di danneggiamento, dispersione o perdita di dati a causa di un uso non corretto o illecito dei sistemi informatici e degli archivi cartacei.

1. ISTRUZIONI GENERALI

1.1. - Segreto professionale o d’ufficio

I “Designati” e gli “Incaricati” al trattamento sono tenuti a mantenere la necessaria riservatezza sulle informazioni di cui vengono a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni di trattamento, evitando di comunicare informazioni e dati a terzi.

Tutto il personale del comparto e della dirigenza – appartenente al ruolo medico, sanitario, tecnico - e chiunque presti la propria attività lavorativa in ambito sanitario (anche in veste di consulente, libero/professionista, tirocinante, volontario, specializzando, personale convenzionato) presso le strutture dell’Azienda è tenuto al segreto professionale o al segreto d’ufficio, ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza di notizie, dati o banche dati di cui - in ragione e in occasione del proprio stato o ufficio - sia venuto a conoscenza. L’eventuale violazione di tale obbligo può comportare l’applicazione di sanzioni di natura deontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quanto previsto dalla legge.

1.2. - Tutela della dignità della persona

Deve essere sempre tutelata la dignità di tutti i soggetti che usufruiscono di prestazioni sanitarie, con particolare riguardo alle fasce deboli (ad es. disabili fisici o psichici, minori e anziani), pazienti sieropositivi o affetti da infezione da HIV, pazienti sottoposti a trattamenti medici invasivi, soggetti particolarmente vulnerabili (ad es. interruzione volontaria di gravidanza o vittime di atti di violenza sessuale o di genere).

Nelle terapie intensive o nei reparti che consentono la visione dei pazienti attraverso sistemi di videosorveglianza sanitaria devono essere utilizzati paraventi o altri accorgimenti che limitino la visibilità dell’interessato, durante l’orario di visita, ai soli familiari e conoscenti.

1.3. - Riservatezza nei colloqui e nel corso di prestazioni sanitarie

Durante i colloqui con l’interessato o con soggetti dallo stesso individuati, o durante l’esecuzione di prestazioni sanitarie, vanno adottate opportune cautele per evitare che le informazioni sulla salute possano essere

conosciute da terzi. Analoghe cautele vanno adottate in occasione della raccolta di dati anamnestici, qualora ciò avvenga in situazioni di promiscuità.

Tutti i professionisti e operatori devono evitare di discutere sulle condizioni cliniche dei pazienti in pubblico, nei luoghi comuni (es. corridoi, bar, ascensore), in presenza di estranei o mediante o utilizzando altre modalità - quali social network, videoconferenza pubblica - ricorrendo a riferimenti che rendano direttamente o indirettamente identificabile la persona.

1.4. – Comunicazioni sulla presenza del Paziente in Ospedale

Utilizzando la modulistica appositamente predisposta, l'interessato – se cosciente e capace – all'atto del ricovero o dell'accesso in Pronto Soccorso deve essere informato e posto in condizione di fornire indicazioni circa i soggetti che possono ricevere notizie sul suo stato di salute e/o sulla sua presenza presso le diverse strutture dell'Azienda.

Deve essere rispettata l'eventuale decisione dell'interessato di non rendere nota la sua presenza in ospedale.

1.5. - Comunicazione all'interessato o a terzi legittimati

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da personale medico o da altro operatore sanitario che intrattenga rapporti diretti con il paziente (ad esempio personale infermieristico autorizzato dal responsabile della Struttura).

Le informazioni sullo stato di salute possono essere fornite a soggetti diversi dall'interessato solo se espressamente individuati dal medesimo, mediante la modulistica in uso, oppure nei casi previsti dalla legge.

Pertanto, prima di dare informazioni a terzi legittimati (ad esempio: coniuge, convivente, figli, genitori, fratelli, ecc.) occorre verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolari soggetti destinatari dell'informazione, accertandosi - per quanto possibile - dell'identità dei soggetti richiedenti.

Nel caso di pazienti minori con genitori separati con affidamento esclusivo, la comunicazione di notizie al genitore non affidatario può avvenire solo previo consenso esplicito di quello affidatario.

Con specifico riferimento alle categorie particolari di dati personali, le notizie da fornire, specie se destinate a soggetti terzi (es. medico di famiglia), devono limitarsi ai soli elementi pertinenti e necessari per le finalità di cura.

1.6. – Rilascio notizie a mezzo telefono o ad organi di stampa

È vietato fornire dati e informazioni di carattere sanitario tramite telefono ad eccezione dei pazienti e delle persone da questi autorizzate e solo se si abbia certezza assoluta dell'identità del chiamante.

Nel caso in cui giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia occorre verificare preliminarmente l'identità del soggetto richiedente richiamando l'interlocutore al numero da questi comunicato.

È fatto divieto di comunicare dati personali o sanitari agli organi di stampa; le eventuali richieste di informazioni devono essere inoltrate alla Direzione Generale per il tramite dell'URP.

1.7. - Distanze di cortesia

Tutti i punti di accettazione e front office devono rispettare una distanza di cortesia, evidenziata da una striscia gialla di segnalazione posta a terra e da un avviso o cartello per l'utenza, sia per operazioni amministrative allo sportello (prenotazione, accettazione, ritiro referti), sia per l'acquisizione di dati personali comuni e sensibili/particolari.

1.8. - Ordine di chiamata

Gli utenti in attesa di visita o di accertamenti (ad es. analisi cliniche o indagini di radiologia) non devono essere chiamati direttamente per nome o cognome ma mediante chiamata non nominativa (eliminacode, numero di prenotazione CUP o attribuzione di un codice numerico o alfanumerico al momento dell'accettazione).

1.9. - Liste di pazienti

È vietata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta.

1.10. - Cartella clinica e documentazione sanitaria

In caso di trasferimento interno dei pazienti ricoverati tra i diversi Presidi o Strutture o nel caso di consulenza o accertamenti diagnostici, la documentazione sanitaria del paziente deve essere riposta in buste o raccoglitori chiusi e non trasparenti, in modo da non permettere la lettura dei dati sensibili da parte di personale non autorizzato.

La documentazione deve essere presa in custodia dal personale sanitario incaricato e da questi consegnata alla struttura di destinazione o restituita alla struttura di provenienza al termine della prestazione o consulenza.

I documenti e i supporti elettronici portati in visione dal paziente devono essere conservati rispettando le regole del rispetto del segreto professionale e, al momento della dimissione o alla conclusione della visita, riconsegnati al paziente.

1.11. - Ritiro referti

Qualsiasi documento relativo ad attività sanitarie (quali referti di esami di laboratorio o di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere consegnato in busta chiusa direttamente all'Interessato.

Il ritiro della documentazione sanitaria è ammesso anche da parte di persona diversa dall'interessato purché munita di delega scritta e con consegna in busta chiusa.

Per gli accertamenti HIV non è consentito il ritiro mediante delega.

1.12. - Attestazione di presenza in ospedale

Le dichiarazioni attestanti la visita, l'esame o il ricovero effettuati (es. giustificativo per il datore di lavoro) devono essere formulate in maniera tale che dalle stesse non possano derivare, per gli estranei, informazioni riguardanti lo stato di salute della persona interessata. L'attestazione deve essere generica e non deve

riportare indicazioni sulla struttura di erogazione, né il timbro con la specializzazione del sanitario o ogni altra informazione da cui si possa evincere la patologia trattata.

2. DOCUMENTAZIONE CARTACEA E SANITARIA

2.1. - Tenuta e custodia

I documenti contenenti dati personali o dati relativi alla salute del Paziente, devono essere custoditi dai “Designati” e dagli “Incaricati” al trattamento in modo da non essere accessibili a persone prive di autorizzazione (es. locali non accessibili al pubblico, armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali o dati relativi alla salute del Paziente non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

In caso di locali aperti al pubblico, le cartelle e i fascicoli devono essere tenuti sulla propria scrivania facendo sì che i dati non siano visibili a persone non autorizzate.

In caso di assenza o allontanamento, anche temporaneo, dalla postazione di lavoro, è vietato lasciare incustoditi fascicoli, cartelle o documenti cartacei contenenti dati relativi alla salute del Paziente. In tal caso occorre chiudere la propria stanza, qualora rimanga incustodita senza personale all’interno, oppure riporre la documentazione in un armadio o cassetto chiuso a chiave.

2.2. - Comunicazione e trasmissione

I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a colleghi che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se tali professionisti o operatori sono a loro volta “Incaricati” al trattamento).

I documenti contenenti dati personali devono essere consegnati ai destinatari utilizzando buste chiuse o raccoglitori sigillati a garanzia dell’integrità - oppure effettuando la consegna personalmente - in modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.

La trasmissione di documentazione sanitaria al domicilio del paziente - su richiesta dello stesso - deve avvenire in busta chiusa ed evitando di riportare sulla busta esterna riferimenti a specifici servizi/strutture dell’Azienda che possano rivelare lo stato di salute dell’interessato o il tipo di patologia.

Nel trasporto della documentazione tra un ufficio e l’altro, occorre adottare precauzioni per evitare la visibilità dei dati personali da parte di estranei (ad es. carpete o faldoni anonimi).

In caso di dati riservati o relativi alla salute occorre accertarsi che il tipo di spedizione sia idoneo a garantire l’integrità della documentazione e la ricezione certa da parte del destinatario.

È proibito trasportare all'esterno del posto di lavoro qualsiasi documentazione contenente dati personali comuni e appartenenti a categorie particolari, salvo motivate esigenze di servizio e fermi restando gli obblighi di custodia.

2.3. - Archiviazione e distruzione

I documenti cartacei contenenti dati sensibili e/o giudiziari devono essere utilizzati dai “Designati” e dagli “Incaricati” al trattamento solo per il tempo necessario allo svolgimento dei relativi compiti istituzionali e poi riposti in archivi o locali ad accesso controllato o, nei casi previsti, affidati al servizio di archiviazione.

Qualora sia necessario disfarsi di documenti cartacei contenenti dati personali, questi devono essere distrutti utilizzando gli appositi distruggidocumenti o, in loro assenza, strappandoli manualmente in modo da non essere più ricomponibili o leggibili.

Allegato 1. 4 – Modello nomina responsabile esterno del trattamento dei dati

NOMINA DEL RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'ART. 28 REG. (UE) 2016/679

TRA

AST MACERATA (in seguito per brevità "Ast" o "Amministrazione"), con sede legale in Macerata (MC) alla via D. Annibali, n. 31, codice fiscale e partita IVA 02095680431 - Titolare del trattamento, nella persona di _____ espressamente delegata dalla Determina n. ____ASTMC del _____ (inserire estremi determina approvazione Regolamento aziendale privacy)

E

_____, con sede in _____, in persona del legale rappresentante p.t. (soggetto individuato quale Responsabile del trattamento) definite congiuntamente "Parti".

Premesso che:

- l'art. 28, par. 3, del Regolamento (UE) n. 2016/679 (General Data Protection Regulation), di seguito anche GDPR, prevede che i trattamenti effettuati per conto del Titolare del trattamento da parte di un Responsabile del trattamento siano regolati da un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la natura e la finalità, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
- l'art. 28 del Regolamento (UE) n. 2016/679 riconosce, altresì, al Titolare del trattamento la facoltà di avvalersi di uno o più responsabili del trattamento dei dati, che abbiano esperienza, capacità, conoscenza per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del regolamento, anche relativamente al profilo della sicurezza;
- le Parti hanno sottoscritto in data _____ un contratto/una convenzione per una durata di _____;
- ai fini del rispetto della normativa europea Regolamento (UE) n. 2016/679 e della normativa interna di attuazione (D.Lgs. 196/2003 – D.Lgs. 101/2018), ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie attività;
- AST Macerata ha affidato alla ditta _____ lo svolgimento delle attività e delle prestazioni così come definite nel contratto sopra citato, che si richiama espressamente, e della quale la presente forma parte integrante e sostanziale;
- tenuto conto delle attività di trattamento necessarie e/o opportune per dare esecuzione agli obblighi concordati tra le Parti, previa valutazione di quanto imposto dal Regolamento UE n. 2016/679, il Titolare ha ritenuto che il Responsabile presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative

adeguate a soddisfare i requisiti del Regolamento UE n. 2016/679 ed a garantire la tutela dei diritti e le libertà degli interessati coinvolti nelle suddette attività di trattamento;

- tale nomina non comporta alcuna modifica della qualifica professionale del Responsabile e/o degli obblighi concordati tra le Parti.

Tutto quanto sopra premesso:

l'AST Macerata,

NOMINA

_____ ai sensi dell'art. 28 del GDPR Responsabile esterno per il trattamento dei dati personali di cui è Titolare l'AST Macerata e di cui il Responsabile può venire a conoscenza nell'esercizio delle attività espletate per conto della stessa relativamente all'adempimento degli obblighi dedotti nel citato contratto/convenzione, affidati dal Titolare al Responsabile.

Articolo 1 - Natura e finalità del trattamento

Il trattamento dei dati personali è effettuato esclusivamente per la corretta esecuzione delle attività concordate tra le Parti e di cui al citato contratto.

Articolo 2 - Categorie di dati personali trattati

Il Responsabile del trattamento per espletare le attività pattuite tra le Parti per conto del Titolare tratta direttamente o anche solo indirettamente le seguenti categorie di dati:

- dati personali, di cui all'art. 4 n. 1 del GDPR, tra i quali:
- dati comuni di cui all'art. 6 del GDPR;
- dati rientranti nelle categorie "particolari" di dati personali (p.e. dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale, all'orientamento sessuale della persona) di cui all'art. 9 del GDPR.

Categorie di interessati cui si riferiscono i dati trattati

Per effetto della presente nomina, le categorie di interessati i cui dati personali possono essere trattati, sono:

- pazienti/utenti;
- familiari dei pazienti/utenti.

Articolo 3 - Obbligo alla riservatezza

Trattandosi di dati personali anche particolari, il responsabile e i propri dipendenti e collaboratori sono tenuti alla assoluta riservatezza analogamente al segreto professionale e al segreto d'ufficio, e comunque a trattare i dati in materia confidenziale e riservata, evitando l'eventuale comunicazione e/o conoscenza da parte di soggetti non autorizzati.

Articolo 4 – Disponibilità e uso dei dati

Qualunque sia la finalità e la durata del trattamento effettuato da parte del Responsabile:

- i dati non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti e dovranno essere restituiti alla conclusione o revoca dell'incarico, o in qualsiasi momento il Titolare ne faccia richiesta;
- il Responsabile si impegna a non vantare alcun diritto sui dati e sui materiali presi in visione.

Coerentemente con quanto prescritto dal GDPR, è esplicitamente fatto divieto al Responsabile di inviare messaggio pubblicitari, commerciali e promozionali, e comunque di contattare gli "interessati" per finalità diverse da quelle nel presente atto.

Articolo 5 - Cessazione del trattamento

Una volta cessati i trattamenti oggetto del contratto/convenzione, salvo rinnovo, il Responsabile si impegna a restituire al Titolare i dati personali acquisiti, pervenuti a sua conoscenza o da questi elaborati in relazione all'esecuzione del servizio prestato e, solo successivamente, si impegna a cancellarli dai propri archivi oppure distruggerli, ad eccezione dei casi in cui i dati debbano essere conservati in virtù di obblighi di legge.

Resta inteso che la dimostrazione delle ragioni che giustificano il protrarsi degli obblighi di conservazione è a carico del Titolare e che le uniche finalità perseguibili con tali dati sono esclusivamente circoscritte a rispondere a tali adempimenti normativi.

Articolo 6 - Validità e Revoca della nomina

La presente nomina avrà validità per tutta la durata del rapporto giuridico intercorrente tra le Parti e potrà essere revocata a discrezione del Titolare.

La presente nomina non costituisce aggravio in capo al Responsabile, rientrando la medesima negli obblighi normativi che regolano i rapporti con il Titolare sotto il profilo della protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 7 - Sub-responsabili

Il Responsabile del trattamento non potrà ricorrere ad altri Responsabili senza la preventiva autorizzazione specifica del Titolare del trattamento. In tale ipotesi il Responsabile dovrà inviare, a mezzo pec, circostanziata e motivata richiesta al Titolare che avrà la facoltà di consentire o meno detta nomina.

Ai sensi dell'art. 28, par. 4 del GDPR, fermo restando quanto previsto al precedente paragrafo, quando un responsabile del trattamento ricorre a un altro responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra Titolare del trattamento e il responsabile del trattamento prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Articolo 8 - Designazione e autorizzazione degli incaricati

Il Responsabile del trattamento garantisce la puntuale individuazione dei soggetti operanti a qualsiasi titolo nella propria organizzazione quali soggetti autorizzati al trattamento.

In particolare, il Responsabile del trattamento si impegna a consentire l'accesso e il trattamento dei dati personali solo a personale debitamente formato e specificamente designato anche ai sensi dell'art. 2-quaterdecies del D.Lgs 196/2003 e s.m.i.

Il Responsabile si impegna ad effettuare per iscritto le nomine e limitare l'accesso e il trattamento ai soli dati personali necessari per lo svolgimento delle attività oggetto del contratto/convenzione.

Il personale autorizzato dovrà ricevere idonea e specifica formazione in relazione al rispetto delle misure organizzative e tecniche, in particolare alle misure di sicurezza adottate, adeguate ad assicurare la tutela dei dati personali trattati nel rispetto delle previsioni normative e della prassi in materia.

Nello specifico il Responsabile:

- individua le persone autorizzate al trattamento dei dati impartendo loro, per iscritto, istruzioni dettagliate in merito alle operazioni consentite e alle misure di sicurezza da adottare in relazione alle criticità dei dati trattati;
- vigila regolarmente sulla puntuale applicazione da parte delle persone autorizzate di quanto prescritto, anche tramite verifiche periodiche;
- garantisce l'adozione dei diversi profili di autorizzazione delle persone autorizzate, in modo da limitare l'accesso ai soli dati necessari alle operazioni di trattamento consentite rispetto alle mansioni svolte;
- verifica periodicamente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione di tutte le persone autorizzate, modificando tempestivamente detto profilo ove necessario (es. cambio di mansione);
- cura la formazione e l'aggiornamento professionale delle persone autorizzate che operano sotto la sua responsabilità circa le disposizioni di legge e regolamentari in materia di tutela dei dati personali.

Il Responsabile, su richiesta, invia al Titolare del trattamento a mezzo pec l'elenco nominativo con specifica evidenza delle relative mansioni dei soggetti autorizzati al trattamento dei dati personali svolti per suo conto e nell'ambito del Contratto.

Articolo 9 – Responsabile della protezione dei Dati

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

Articolo 10 - Diritti degli interessati

Premesso che l'esercizio dei diritti riconosciuti all'interessato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Titolare, il Responsabile si rende disponibile a collaborare con il Titolare stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.

Il Responsabile si impegna ad assistere il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare e di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

In particolare, il Responsabile dovrà comunicare al Titolare, senza ritardo e comunque non oltre le 72 ore dalla ricezione, le istanze eventualmente ricevute e avanzate dagli interessati in virtù dei diritti previsti dalla vigente normativa (es. diritto di accesso, ecc.) e a fornire le informazioni necessarie al fine di consentire al Titolare di evadere le stesse entro i termini stabiliti dalla normativa.

Articolo 11 - Registro dei trattamenti

Il Responsabile mantiene un registro (in forma scritta e/o anche in formato elettronico) di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, contenente:

- il nome e i dati di contatto del Responsabile e/o dei suoi Sub Responsabili;
- le categorie dei trattamenti effettuati per conto del Titolare;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate adottate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, par. 1 del GDPR.

Il Responsabile garantisce, inoltre, di mettere a disposizione del Titolare e/o dell'Autorità di controllo che ne dovessero fare richiesta, il suddetto registro dei trattamenti.

Il Responsabile si impegna a coadiuvare il Titolare nella redazione del proprio Registro delle attività di trattamenti, segnalando anche, per quanto di propria competenza, eventuali modifiche da apportare al Registro.

Articolo 12 - Sicurezza dei dati personali

Il Responsabile è tenuto, ai sensi dell'art. 32 del GDPR, ad adottare le necessarie e adeguate misure di sicurezza (eventualmente anche ulteriori rispetto a quelle nel seguito indicate) in modo tale da ridurre al minimo i rischi di distruzione accidentale o illegale, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, conservati o comunque trattati, o il trattamento non conforme alle finalità della raccolta.

Il Responsabile fornisce al Titolare l'elenco delle adeguate misure di sicurezza adottate.

Articolo 13 - Sicurezza e Amministrazione del Sistema (ADS)

Il Responsabile fornirà al Titolare la lista nominativa degli ADS, con questi intendendo le persone fisiche che svolgono per conto del Responsabile ed in esecuzione dei compiti concordati ed affidati dal Titolare, attività di gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i software complessi che trattano dati, le reti locali e gli apparati di sicurezza di quest'ultimo, o comunque che possano intervenire sulle misure di sicurezza a presidio dei

medesimi dati. Con riferimento ai soggetti individuati, il Responsabile deve comunicare rispetto ad ognuno i compiti e le operazioni svolte.

Articolo 14 - Compiti e istruzioni per il Responsabile

Il Responsabile ha il potere ed il dovere di trattare i dati personali indicati nel rispetto della normativa vigente, attenendosi sia alle istruzioni di seguito fornite, sia a quelle che verranno rese note dal Titolare mediante procedure e/o comunicazioni specifiche.

Il Responsabile dichiara espressamente di comprendere ed accettare le istruzioni di seguito rappresentate e si obbliga a porre in essere, nell'ambito dei compiti contrattualmente affidati, tutti gli adempimenti prescritti dalla normativa di riferimento in materia di tutela dei dati personali al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non consentito o non conforme alla raccolta.

Articolo 15 - Modalità di trattamento e requisiti dei dati personali

Il Responsabile si impegna:

- a trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. – specificamente designati incaricati del trattamento – i dati personali per le sole finalità connesse allo svolgimento delle attività previste dal contratto/convenzione, in modo lecito e secondo buona fede e correttezza, nonché nel pieno rispetto delle disposizioni previste dal GDPR, nonché, infine, dalle presenti istruzioni;
- non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto - i dati personali ricevuti dal Titolare e o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare stesso, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;
- collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
- dare immediato avviso al Titolare in caso di cessazione dei trattamenti concordati;
- non creare banche dati nuove senza espressa autorizzazione del Titolare, fatto salvo quando ciò risulti strettamente indispensabile ai fini dell'esecuzione degli obblighi assunti;
- in caso di ricezione di richieste specifiche avanzate dall'Autorità Garante per la protezione dei dati personali o altre autorità, a coadiuvare il Titolare per quanto di sua competenza;
- segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;
- coadiuvare, su richiesta, il Titolare ed i soggetti da questo indicati nella redazione della documentazione necessaria per adempiere alla normativa di settore, con riferimento ai trattamenti di dati effettuati dal Responsabile in esecuzione delle attività assegnate.

Articolo 16 - Istruzioni specifiche per il trattamento dati particolari

Il Responsabile deve:

- verificare la corretta osservanza delle misure previste dal Titolare in materia di archiviazione nel rispetto di quanto previsto dal precedente articolo 6, potendo derivare gravi conseguenze da accessi non autorizzati alle informazioni oggetto di trattamento;
- prestare particolare attenzione al trattamento dei dati personali rientranti nelle categorie particolari degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura;
- conservare, nel rispetto di quanto previsto dal precedente articolo 6, la documentazione contenente dati particolari adottando misure idonee al fine di evitare accessi non autorizzati ai dati, distruzione, perdita e/o qualunque violazione di dati personali;
- vigilare affinché i dati personali degli interessati vengano comunicati solo a quei soggetti preventivamente autorizzati dal Titolare (ad esempio a propri fornitori e/o subfornitori) che presentino garanzie sufficienti secondo le procedure di autorizzazione disposte e comunicate dal Titolare. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici;
- sottoporre preventivamente al Titolare, per una sua formale approvazione, le richieste di dati da parte di soggetti esterni;
- non diffondere i dati personali, comuni e particolari, degli interessati;
- segnalare eventuali criticità nella gestione della documentazione contenente dati personali particolari al fine di consentire idonei interventi da parte del Titolare.

Articolo 17– Violazione dei dati

Il Responsabile si impegna a notificare al Titolare, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore, con comunicazione da inviarsi all'indirizzo pec del Titolare, ogni violazione dei dati personali (data breach) fornendo, altresì:

- la descrizione della natura della violazione e l'indicazione delle categorie dei dati personali e il numero approssimativo di interessati coinvolti;
- comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze;
- la descrizione delle misure adottate o di cui dispone per porre rimedio alla violazione o, quantomeno, per attenuarne i possibili effetti negativi.

Fermo quanto sopra previsto, il Responsabile si impegna a prestare ogni più ampia assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 33 - 34 del GDPR.

Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, su richiesta, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi, al riguardo anche avvalendosi dell'operato di subfornitori.

Articolo 18 - Valutazione di impatto e consultazione preventiva

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

Articolo 19 - Trasferimento dei dati personali

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

Articolo 20 - Attività di audit

Il Responsabile si impegna a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del presente atto e del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da esso incaricato.

Qualora il Titolare rilevasse comportamenti difformi a quanto prescritto dalla normativa in materia nonché dalle disposizioni contenute nei provvedimenti del Garante per la protezione dei dati personali, provvederà a darne comunicazione al Responsabile, senza che ciò possa far venire meno l'autonomia dell'attività di impresa del Responsabile ovvero possa essere qualificato come ingerenza nella sua attività.

Articolo 21 - Ulteriori istruzioni

Il Responsabile comunica tempestivamente al Titolare qualsiasi modificazione di assetto organizzativo o di struttura proprietaria che dovesse intervenire successivamente all'affidamento dell'incarico, affinché il Titolare possano accertare l'eventuale sopravvenuta mancanza dei requisiti previsti dalla vigente normativa o il venir meno delle garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate per il corretto trattamento dei dati oggetto della presente nomina.

Il Responsabile informa prontamente il Titolare delle eventuali carenze, situazioni anomale o di emergenza rilevate nell'ambito del servizio erogato - in particolare ove ciò possa riguardare il trattamento dei dati personali e le misure di sicurezza adottate dal Responsabile - e di ogni altro episodio o fatto rilevante che intervenga e che riguardi comunque l'applicazione del GDPR (ad es. richieste del Garante, esito delle ispezioni svolte dalle Autorità, ecc.) o della normativa nazionale ancorché applicabile

Articolo 22 – Norme finali e responsabilità

Il Titolare, poste le suddette istruzioni e fermi i compiti sopra individuati, si riserva, nell'ambito del proprio ruolo, di impartire per iscritto eventuali ulteriori istruzioni che dovessero risultare necessarie per il corretto e conforme svolgimento delle attività di trattamento dei dati collegate all'accordo vigente tra le Parti, anche a completamento ed integrazione di quanto sopra definito.

Il Responsabile dichiara sin d'ora di mantenere indenne e manlevato il Titolare da qualsiasi danno, onere, spesa e conseguenza che dovesse loro derivare a seguito della violazione, da parte del Responsabile o di suoi Sub – Responsabili, degli impegni relativi al rispetto della disciplina in materia di protezione dei dati personali o delle istruzioni contenute nei relativi atti di nomina anche in seguito a comportamenti addebitabili ai loro dipendenti, rappresentanti, collaboratori a qualsiasi titolo.

Il presente atto di nomina viene sottoscritto dalle parti digitalmente.

Per AST Macerata

Il _____

Per _____

Il legale rapp.te
