ASP
PALERMO
AZIENDA SANITARIA PROVINCIALE

Sede legale: Via G. Cusmano, 24 – 90141 PALERMO
C.F. e P. I.V.A.: 05841760829

AZIENDA SANITARIA PROVINCIALE DI PALERMO

REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

sulla base del Regolamento Europeo 2016/679 e del D. Lgs. 196/2003 modificato dal D. Lgs. 101/2018

Redazione a cura della U.O.S. DATA Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali

Data Ultimo Aggiornamento Giugno 2024

SOMMARIO

DISPOSIZIONI GENERALI

ART. 1 - OGGETTO E FINALITÀ

Il presente Regolamento disciplina, per l'Azienda Sanitaria Provinciale di Palermo (di seguito: "ASP - PA", "Azienda" o il "Titolare"), la tutela delle persone fisiche e degli altri soggetti con riguardo al trattamento dei dati personali e alle norme relative alla libera circolazione dei dati, nel rispetto di quanto previsto dal D.lgs. n. 196/2003 ("Codice in materia di protezione dei dati personali" di seguito "Codice") – come modificato dal D.Lgs. 101/2018 – e dal Regolamento UE 2016/679 (di seguito Regolamento UE o GDPR)

Lo scopo del presente Regolamento è di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda Sanitaria Provinciale di Palermo.

La Azienda Sanitaria Provinciale di Palermo adotta misure tecniche e organizzative per garantire un livello di sicurezza adeguato ai rischi di distruzione o perdite, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi degli articoli di cui al Capo 3 del Regolamento UE.

ART. 2 - AMBITO DI APPLICAZIONE ED EFFICACIA

Il presene Regolamento si applica con efficacia immediata a tutti i trattamenti di dati personali interamente o parzialmente automatizzati e/o non automatizzati contenuti in archivi o destinati a figurarvi effettuati nell'ambito delle attività svolte dalle strutture che operano sotto la titolarità della ASP – PA o per conto di essa ovvero alla rete ospedaliera (i Presidi Ospedalieri), alla rete territoriale (i Distretti), ai Dipartimenti, all'area Amministrativa dell'Azienda e a tutti gli ulteriori servizi, strutture ed uffici aziendali, come individuate dall'Atto Aziendale adottato con Deliberazione n° 81 del 21 gennaio 2020 e ss.mm.ii.,in grado di garantire un elevato livello di performance nell'esecuzione e gestione operativa quotidiana di una efficace governance dei dati personali delle persone fisiche, degli obblighi di tutela dei diritti e della dignità dell'interessato tipici di un'entità che opera in un ambiente sanitario quale è l'Azienda Sanitaria Provinciale di Palermo.

ART. 3 - DEFINIZIONI, ACRONIMI E ABBREVIAZIONI

Ai fini del presente Regolamento, in base a quanto previsto dalla normativa vigente in materia di Protezione dei Dati Personali, si riportano le seguenti definizioni:

3.1 DEFINIZIONI

- **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.
- **Autorità di controllo**: Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR. In Italia è costituita dall'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy).
- **Autorizzato al Trattamento**: La persona fisica che ha accesso ai dati e compie le operazioni di trattamento sotto la diretta autorità del Titolare del trattamento e/o del Responsabile del trattamento e/o del Designato/Delegato del Trattamento..
- **Codice Privacy**: Decreto Legislativo del 30 giugno 2003, n.196, recante il "Codice in materia di protezionedei dati personali" come integrato dalle modifiche introdotte dal decreto legislativo 10 agosto 2018,n.101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679. Di seguito, per brevità, Codice.

- **Comunicazione**: Si intende il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2 -quaterdecies, 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; (Art. 2.Modifiche alla parte I, titolo I,del decreto legislativo 30 giugno 2003, n. 196, comma 4,lett. a) del D.lgs. n.101/ 18).
- **Consenso dell'Interessato**: Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. (art. 4 Definizioni, Par. 11) del GDPR).
- **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. (art. 4 Definizioni, Par. 1) del GDPR).
- **Dati Personali relativi a Categorie Particolari**: Ai sensi dell'art. 9, par. 1 del GDPR: si intendono i 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.
- **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 (art. 4 Definizioni, Par. 15) del GDPR).
- **Dati relativi a Condanne Penali e Reati**: I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4 Definizioni, comma 1, lett. d) del Codice) – definizione abrogata. I dati giudiziari nel GDPR sono identificabili con i dati personali relativi a condanne penali e reati (art. 10 del GDPR).
- **Dati Biometrici**: Si intendono 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 (art. 4 Definizioni, Par. 14) del GDPR).
- **Dati Genetici**: Si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4 Definizioni, Par. 13) del GDPR).
- **Dati Anonimi**: i dati che in origine, o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile;
- **Delegato/Designato al Trattamento**: la persona fisica cui il Titolare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, attribuisce specifici compiti e funzioni connessi al trattamento di dati personali.
- **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.
- **Diffusione**: Si intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (Art. 2. Modifiche alla parte I, titolo I,del decreto legislativo 30 giugno 2003, n. 196, comma 4, lett. b) del D.lgs. n.101/ 18).

- **Garante per la Protezione dei Dati Personali**: L'Autorità di controllo italiana (l'Autorità Garante per la protezione dei Dati personali) designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679.
- **GDPR o RGPD**: General Data Protection Regulation o Regolamento per la Protezione dei Dati Personali, di cui al Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, di seguito, in breve, Regolamento UE.
- **Interessati**: Le persone fisiche cui i Dati Personali si riferiscono.
- **Limitazione di Trattamento**:il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
- **Privacy Policy**: Sezione del sito web istituzionale ove è possibile consultare ogni indicazione utile, per la protezione dei dati personali, fornita dal Titolare di Trattamento. https://www.aspalermo.org - alla voce privacy.
- **Profilazione:** qualsiasi forma di trattamento automatizzato (raccolta e analisi) 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.
- **Pseudonimizzazione**: il trattamento dei dati personali in modo tale che gli stessi 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.
- **Registro delle Attività di Trattamento**: Ai sensi dell'art.30 del Regolamento UE 2016/679 l'ASP - PA redige, conserva e aggiorna il Registro delle Attività di Trattamento che contiene la rilevazione di tutti i trattamenti di dati personali che vengono effettuati nello svolgimento della propria attività istituzionale. Il Registro è depositato presso l'Azienda Sanitaria Provinciale di Palermo a disposizione, su richiesta, dell'Autorità Garante per la protezione dei dati personali.
- **Responsabile per la Protezione dei Dati (R.P.D.), o Data Protection Officer (D.P.O.) :** Soggetto nominato dal Titolare o dal Responsabile del Trattamento, ai sensi dell'art. 37 del GDPR, (Designazione del Responsabile della Protezione dei Dati) cui sono affidati i compiti previsti nell'art. 39 dello stesso GDPR. e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati.
- **Responsabile del Trattamento** : la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- **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; (art. 4 Definizioni, Par. 7) del GDPR).
- **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 (art. 4 Definizioni, Par. 2) del GDPR).
- **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.

- **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.

3.2 - ACRONIMI, ABBREVIAZIONI
Ai fini del presente documento, si identificano i seguenti acronimi, abbreviazioni.

CODICE:	**TITOLO:**
AdS:	Amministratore di Sistema
ASP – PA	Azienda Sanitaria Provinciale di Palermo
DPIA	Data Protection Impact Assessment
GDPR	General Data ProtectionRegulatin
RPD/DPO	Responsabile per la Protezione dei Dati/Data Protection Officer
UOC	Unità Operativa Complessa
UOS	Unità Operativa Semplice
UOSD	Unità Operativa Semplice Dipartimentale

ART. 3.3 - RIFERIMENTI NORMATIVI
- **REGOLAMENTO (UE) 2016/679** 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 (regolamento generale sulla protezione dei dati).
- **Decreto legislativo 30 giugno 2003, n. 196 CODICE** IN MATERIA DI PROTEZIONE DEI DATI PERSONALI e successive modificazioni ed integrazioni, come novellato dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101.
- **DECRETO LEGISLATIVO 10 agosto 2018, n. 101** Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 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 (regolamento generale sulla protezione dei dati).
- **PROVVEDIMENTO 5 giugno 2019 del Garante** per la Protezione dei Dati Personali. Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'articolo 21, comma 1 del decreto legislativo 10 agosto 2018, n. 101. (Provvedimento n. 146). (19A04879) (GU Serie Generale n.176 del 29-07-2019).
- **PROVVEDIMENTO** Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) e successive modificazioni (così modificato in base al provvedimento del 25 giugno 2009).
- **GUIDA del GARANTE PRIVACY** italiano all'applicazione del Regolamento Europeo in materia di protezione dei dati personali.

ART. 4 - TRATTAMENTO DI DATI PERSONALI

- Con l'espressione "**trattamento**", ai sensi dell'art. 4, GDPR , deve intendersi 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;
- I trattamenti da effettuarsi da parte delle strutture della ASP - PA devono essere effettuati esclusivamente per l'esercizio delle funzioni istituzionali dell'Azienda e con finalità compatibili con tali funzioni, con particolare riferimento all'ambito sanitario;
- Tutti i trattamenti di dati personali effettuati dalla ASP - PA devono rispettare i principi di trattamento di cui al successivo articolo 6 del presente Regolamento.
- Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento, dei Responsabili, dei soggetti Delegati/Designati e dei soggetti Autorizzati al trattamento dei dati personali. Non è consentito il trattamento di dati personali da parte di persone non autorizzate.
- Il trattamento dei dati personali raccolti direttamente dall'ASP - PA o ad essa comunicati da altri soggetti è effettuato sia con che senza l'ausilio di strumenti elettronici.
- I trattamenti effettuati dall'ASP - PA, concernenti i dati personali, sono finalizzati prevalentemente all'erogazione delle prestazioni sanitarie, nonché all'espletamento dei compiti attribuiti dal Servizio Sanitario Nazionale ed agli adempimenti amministrativi e contabili di organizzazione e di controllo preordinati alla predetta erogazione, come regolamentati dalla Legge 833/78, dal D.Lgs. 502/92 e ss.mm.ii., dal DL 13 settembre 2012 n.158 convertito nella Legge 8 novembre 2012 n.189 – Legge Balduzzi oltre che da tutta la normativa applicabile allo specifico settore di appartenenza.

A titolo esemplificativo e non esaustivo, le macro-categorie di trattamento possono essere classificate nel seguente elenco:

- prevenzione collettiva e di sanità pubblica, anche a supporto delle Autorità Sanitarie;
- diagnostica strumentale e di laboratorio;
- prevenzione delle malattie, cura e riabilitazione in regime ambulatoriale sia in sede distrettuale che ospedaliera;
- ricovero ordinario, in day surgery ed in day hospital;
- ricovero in regime residenziale e semiresidenziale;
- prestazioni sanitarie a rilevanza sociale;
- attività o servizi socio-assistenziali su delega dei singoli enti locali;
- medicina legale;
- ricerca e sperimentazione, nonché elaborazione statistica, epidemiologica e sociologica.

Sono altresì effettuati nell'ambito dell'ASP – PA i trattamenti di dati personali previsti da norme legislative e regolamentari concernenti:

- la gestione del personale dipendente, ivi comprese le procedure di assunzione;
- la gestione dei soggetti che intrattengono rapporti giuridici con la ASP - PA, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Azienda stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i tirocinanti, i volontari;
- la gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni e servizi (anche di natura informatica e di Ingegneria Clinica), nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
- la gestione dei rapporti con i soggetti accreditati o convenzionati, associazioni anche di volontariato ed altri Enti ed Organismi Pubblici;

- la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

L'elenco dei macro-ambiti di trattamento previsti dalle funzioni istituzionali in ambito aziendale può essere sintetizzato nel seguente elenco:

- Tutela dai rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro
- Sorveglianza epidemiologica delle malattie infettive e diffusive e delle tossinfezioni alimentari
- Attività amministrative e certificatorie correlate alle vaccinazioni e alla verifica assolvimento obbligo vaccinale
- Attività amministrative correlate ai programmi di diagnosi precoce
- Attività fisica e sportiva
- Attività di assistenza socio-sanitaria a favore di fasce deboli di popolazione e di soggetti in regime di detenzione
- Medicina di base – pediatria di libera scelta – continuità assistenziale (ex guardia medica notturna e festiva, guardia turistica).
- Assistenza sanitaria di base: riconoscimento del diritto all'esenzione per patologia/invalidità/reddito e gestione archivio esenti
- Assistenza sanitaria di base: assistenza sanitaria in forma indiretta
- Cure all'estero urgenti e programmate
- Assistenza sanitaria di base: assistenza agli stranieri in Italia (particolari categorie)
- Assistenza integrativa
- Assistenza protesica
- Assistenza domiciliare programmata e integrata
- Attività amministrative correlate all'assistenza a soggetti non autosufficienti, a persone con disabilità fisica, psichica e sensoriale e a malati terminali nei regimi residenziale, semiresidenziale ambulatoriale (ex art. 26 della L. 833/1978) e domiciliare
- Assistenza termale
- Attività amministrativa, programmatoria, gestionale e di valutazione relativa all'assistenza ospedaliera in regime di ricovero
- Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività Immunotrasfusionale
- Attività amministrativa, programmatoria gestionale e di valutazione concernente la donazione, il trapianto di organi, tessuti e cellule
- Soccorso sanitario di emergenza/urgenza sistema "118". Assistenza sanitaria di emergenza
- Attività amministrative correlate ad assistenza specialistica, ambulatoriale e riabilitazione.
- Promozione e tutela della salute mentale
- Attività sanitarie e amministrative correlate alle dipendenze: tossicodipendenza, alcolismo, farmacodipendenza, gioco d'azzardo, tabagismo, HIV (solo per gli aspetti psico-sociali)
- Assistenza socio-sanitaria per la tutela della salute materno-infantile ed esiti della gravidanza
- Attività amministrative correlate all'assistenza farmaceutica territoriale e ospedaliera
- Sperimentazione Clinica
- Farmacovigilanza e rilevazione reazioni avverse a vaccini e farmaci
- Attività amministrative correlate all'erogazione a totale carico del servizio sanitario nazionale, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dall'Agenzia Italiana del Farmaco
- Attività amministrative correlate all'assistenza a favore delle categorie protette (morbo di Hansen).
- Attività amministrativa programmatoria, gestionale e di valutazione concernente l'assistenza ai nefropatici cronici in trattamento dialitico
- Attività medico-legale inerente l'istruttoria delle richieste di indennizzo per danni da vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati

- Attività medico-legale inerente gli accertamenti finalizzati al sostegno delle persone con disabilità (riconoscimento dello stato di invalidità, cecità e sordità civili, della condizione di handicap ai sensi della L. 104/92, accertamenti per il collocamento mirato al lavoro delle persone con disabilità ai sensi della L. 68/99)
- Attività medico-legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego: idoneità allo svolgimento di attività lavorative; controllo dello stato di malattia dei dipendenti pubblici e privati; accertamenti sanitari di assenza di tossicodipendenza o di assunzione di sostanze stupefacenti o psicotrope in lavoratori addetti a mansioni che comportino particolari rischi per la sicurezza, l'incolumità e la salute di terzi)
- Attività medico-legale inerente l'accertamento dell'idoneità al porto d'armi, ai fini della sicurezzasociale
- Attività medico-legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
- Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza delle infermità da causa di servizio
- Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari e consulenze e pareri in materia di bioetica
- Attività medico-legale in ambito necroscopico
- Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
- Attività amministrative correlate alla gestione e verifica sull'attività delegata a soggetti accreditati o convenzionati del SSN
- Gestione Risorse Umane e Trattamento Economico del Personale
- Attività medico-legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
- Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza delle infermità da causa di servizio
- Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari e consulenze e pareri in materia di bioetica
- Attività medico-legale in ambito necroscopico
- Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
- Attività amministrative correlate alla gestione e verifica sull'attività delegata a soggetti accreditati o convenzionati del SSN
- Gestione Risorse Umane e Trattamento Economico del Personale

L'elenco completo dei trattamenti effettuati dall'ASP - PA è inserito nel Registro dei Trattamenti secondo quanto previsto dall'Art. 30 del GDPR; tale elenco deve essere puntualmente aggiornato dal Titolare e dai Soggetti Delegati/Designati al Trattamento dei dati in base alla propria area di competenza e di responsabilità.

Qualora un trattamento di dati personali venga affidato in tutto o in parte a soggetti esterni (es.:Responsabili del Trattamento), deve essere previsto, nell'ambito del documento di accordo, il riferimento allo specifico trattamento previsto nel Registro Aziendale dei Trattamenti di Dati Personali.

ART. 5 - PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

La ASP – PA in qualità di Titolare del trattamento, secondo quanto previsto dal principio di responsabilizzazione, è competente per il rispetto dei principi di trattamento di seguito elencati:

- **Liceità, Correttezza e Trasparenza**: i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **Limitazione della Finalità**: i dati personali devono essere 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, conformemente all'articolo 89, paragrafo 1 del GDPR, considerato incompatibile con le finalità iniziali;
- **Minimizzazione dei Dati**: i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Esattezza**: i dati personali devono essere 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;
- **Limitazione della Conservazione**: i dati personali devono essere 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 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato;
- **Integrità e Riservatezza**: i dati personali devono essere 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.

ART. 6 - CRITERI PER L'ESECUZIONE DEL TRATTAMENTO DEI DATI PERSONALI

- Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e delle libertà fondamentali delle persone fisiche nonché delle norme relative alla libera circolazione di tali dati.
- Oggetto del trattamento devono essere solo i dati essenziali per lo svolgimento delle attività istituzionali nel rispetto del ''**Principio di Minimizzazione''** come previsto dall'art. 7 del presente Regolamento.
- I dati personali devono essere trattati in modo lecito, corretto e trasparente, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati nel rispetto dei principi previsti dall'art. 5 del presente Regolamento. Le condizioni di liceità ammissibili per i trattamenti dei dati personali effettuati dalle strutture della ASP - PA sono stabilite nell'art. 7 del presente Regolamento.
- Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi nel rispetto dall'art. 25 del GDPR "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita".
- È compito delle persone fisiche Delegate/Designate al trattamento dei dati personali, ai sensi dell'art. 2-quaterdecies del D. lgs. 196/203 e ss.mm.ii., in conformità con il Regolamento (UE) 2016/679 censire e verificare periodicamente la liceità e la correttezza dei trattamenti nell'ambito della propria area di competenza, verificarne l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità

perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa

- I dati che, anche a seguito di verifiche effettuate dai Delegati/Designati al Trattamento dei Dati o dal R.P.D./D.P.O., risultassero eccedenti, non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione dell'atto che li contiene, a norma di legge.
- I trattamenti di dati effettuati impiegando banche dati di più titolari diversi dall'ASP – PA (interconnessione di banche dati) sono utilizzati nelle sole ipotesi previste da espressa disposizione di legge.
- Ai sensi dell'art. 9 del GDPR, i dati personali appartenenti a particolari categorie sono conservati, ove possibile, in base ad opportune misure tecniche e organizzative applicabili secondo i criteri stabiliti dall'art. 32 del GDPR, separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.
- In ogni caso devono essere adottate misure tecniche e organizzative tali da garantire che i dati personali siano accessibili alle sole persone fisiche autorizzate al trattamento dei dati personali e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

ART. 7 - CONDIZIONI DI LICEITÀ

1. Le condizioni di liceità, in presenza delle quali il Titolare compie operazioni di trattamento dei dati personali sono quelle indicate nell'art. 6.1 del Regolamento UE 2016/879 come di seguito riportate:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- 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;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- 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;

2. Come previsto dall'art. 6.3 lett. b) del GDPR, secondo quanto disposto dall'art. 2-ter del D.Lgs. 196/03, il 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 – rif. Punto n°1 del presente articolo – deve essere basato su una norma di legge o, nei casi previsti dalla legge che contempli l'adozione di un Regolamento.
Pertanto, per i trattamenti fondati su tale base giuridica, è necessaria l'individuazione specifica della legislazione di riferimento da indicarsi nel Registro Aziendale dei Trattamenti.

3. Ai sensi dell'art. 9.2 del GDPR, è possibile effettuare il trattamento di particolari categorie di dati Personal i (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), in base alle seguenti basi giuridiche applicabili al contesto delle attività svolte per fini istituzionali dalla ASP – PA :

- 9.2.a) del GDPR: 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 disponga che tale base giuridica (consenso) non sia applicabile;
- 9.2.b) del GDPR: 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;

- 9.2.c) del GDPR: 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;
- 9.2.f) del GDPR: il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogni qualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- 9.2.g) del GDPR: 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;
- 9.2.h) del GDPR: il trattamento è necessario per **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (di seguito "finalità di cura"** come indicato dal Garante nel Provvedimento n. 55 del 7 marzo 2019)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. Tale base giuridica prevede anche il caso di trattamento di particolari categorie di dati personali anche per finalità di medicina del lavoro, valutazione della capacità lavorativa del dipendente
- 9.2.i) del GDPR: 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;
- 9.2.j) del GDPR: 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 allaprotezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

4. Per trattamenti per "**finalità di cura",** sulla base dell'art. 9, par. 2, lett. h) e par. 3 del GDPR, sono propriamente quelli effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza.
5. Per trattamenti di dati personali di cui all'art. 9, par. 2, lett. h) del GDPR, si intendono quelli "necessari"al perseguimento delle specifiche "finalità di cura" previste dal GDPR, cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute.
6. Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi,eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del GDPR).
7. I trattamenti delle **categorie particolari di dati** personali necessari per motivi di interesse pubblico rilevante ai sensi dell'articolo 9.2, lettera g) del GDPR 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 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 (art. 2-sexies c.1 del D.lgs. 196/2003).
8. Fermo quanto previsto dal precedente comma, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati dell'ASP - PA, nell'ambito dello svolgimento di compiti di

interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie indicate dall'art. 2-sexies c.2) del D.lgs. 196/2003.

9. I trattamenti di dati personali relativi a condanne penali e reati, come previsti dall'art. 10 del GDPR, sono regolamentati dallo stesso e dall'articolo 2-octies del D.lgs. 196/2003. Il trattamento per tali dati "deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

10. Secondo quanto previsto dall'articolo 2-quater c.4) del D.lgs. 196/2003 il rispetto delle disposizioni contenute nelle regole deontologiche promosse dall'Autorità Garante per la Protezione dei Dati costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.

ART. 8 - COMUNICAZIONE E DIFFUSIONE DEI DATI

1. La comunicazione da parte dell'ASP – PA ad altri Titolari di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del Regolamento UE e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento UE, è lecita nei seguenti casi:

a) si basa sul consenso dell'interessato;
b) è necessaria all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) è necessaria per adempiere un obbligo legale al quale è soggetta la ASP - PA;
d) è necessaria per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) è necessaria per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita la ASP - PA.

2. La comunicazione di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'art. 9 del Regolamento UE e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento UE, nei casi previsti dal punto 1 lett. c) ed e) del presente articolo, da parte dell'ASP – PA ad altri titolari è ammessa solo quando sia prevista da una norma di legge o nei casi previsti da una legge che contempli l'adozione di un regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di 45 giorni dalla data di comunicazione obbligatoriamente preventiva al Garante e non sia stata adottata dall'Autorità diversa determinazione

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste da una norma di legge o, nei casi previsti dalla legge che contempli l'adozione di un regolamento.

4. I dati genetici, biometrici e relativi alla salute, possono essere oggetto di comunicazione in presenza di una delle condizioni previste dall'art. 7 del presente Regolamento ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dall'articolo 2-septies del Codice;

5. I dati genetici, biometrici e relativi alla salute non possono essere diffusi secondo quanto previsto dall'art. 2-septies del Codice.

6. La comunicazione e la diffusione dei dati per finalità di ricerca scientifica o di statistica, sono consentite qualora si tratti di dati anonimi e comunque tali da non consentire l'identificazione degli interessati.

7. Il trasferimento di dati personali verso Stati appartenenti all'Unione Europea, è consentito nel rispetto di quanto previsto nei commi precedenti, senza necessità di autorizzazione del Garante.

8. Qualora i dati personali siano oggetto di trasferimento verso Stati non appartenenti all'Unione Europea, debbono essere osservate le ulteriori cautele previste dal Regolamento UE 2016/679.

9. Ulteriori precisazioni sono specificate nella Procedura Aziendale di Gestione delle Informative e dei Consensi, allegata al presente Regolamento, e nella normativa vigente applicabile.

ART. 9 - INFORMAZIONE TRASPARENTE

L'ASP di Palermo, quale Titolare del Trattamento, adotta misure appropriate per fornire all'interessato tutte le informazioni e comunicazioni riguardanti il trattamento dei dati in forma concisa, trasparente intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni rivolte specificatamente ai minori.
Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
L'ASP - PA a tal riguardo predispone specifiche informative sul trattamento dei dati personali che riportano le informazioni previste dalla vigente normativa secondo quanto disposto dagli artt. 13 e 14 del Regolamento UE 2016/679 relativamente a:

- Identità e i dati di contatto del Titolare del trattamento e del Responsabile della Protezione dei Dati;
- Finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- Destinatari cui possono essere comunicati i dati;
- Periodo di Conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- Esistenza del Diritto dell'Interessato di chiedere al Titolare del Trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- Qualora il trattamento sia basato sull'art. 6, paragrafo 1, lettera a), oppure sull'art. 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- Diritto di proporre Reclamo al Garante della Privacy;
- Comunicazione di dati personali basata su un obbligo legale o contrattuale;
- Esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
- Fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

L'informativa all'interessato viene fornita per iscritto, anche per estratto, tramite materiale informativo reso disponibile in luoghi comuni dell'ASP di Palermo e presso l'apposita sezione"Privacy" del sito web aziendale www.asppalermo.org (**Allegato n°1**)
Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'ASP di Palermo, è predisposta separata informativa, consultabile sul sito webb dell'ASP – PA, alla pagina privacy.
L'informativa sul Trattamento dei dati personali non viene rilasciata all'interessato nel caso in cui questi disponga già delle sopra indicate informazioni o nel caso in cui comunicarle risulti impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, purché in tali casi siano state adottate preventivamente misure tecniche e organizzative adeguate per la protezione dei dati specie al fine di garantire il rispetto del principio della minimizzazione dei dati, e ulteriori misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato.
Qualora l'ASP di Palermo 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 e ogni ulteriore informazione pertinente

ART. 10 – DIRITTO ALL'ANONIMATO

L'ASP – PA 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.

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 – AUTORIZZAZIONE AL TRATTAMENTO DEI DATI

- In conformità ai contenuti del Provvedimento n. 55/2019 dell'Autorità Garante per la protezione dei dati personali "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – 7 marzo 2019", l'ASP - PA assicura la piena applicazione del principio in base al quale, nel caso di trattamenti di dati personali per "**finalità di cura**" effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza**, non viene richiesto il consenso del paziente**; ciò in quanto trattasi di attività di trattamento di dati personali necessari alla prestazione sanitaria richiesta dall'interessato.
- Sono da intendersi necessari alla prestazione sanitaria richiesta dall'interessato anche i trattamenti di dati personali connessi alle attività amministrativo/contabili che l'ASP - PA, ai sensi di disposizioni di legge o di regolamento, è tenuto ad effettuare in qualità di soggetto pubblico operante nell'ambito del Servizio Sanitario Regionale e che, appunto, in quanto tali, non richiedono - parimenti a quelli di cui al precedente comma - l'acquisizione del consenso dell'interessato.
- Diversamente, i trattamenti di dati personali attinenti solo in senso lato alla cura - ma non strettamente necessari anche se effettuati da professionisti sanitari - richiedono una distinta base giuridica da individuarsi nel consenso o in altro presupposto di liceità.
- Per quanto concerne l'individuazione dei trattamenti di dati personali in ambito sanitario che richiedono il consenso esplicito dell'interessato, l'ASP – PA ha recepito le indicazioni fornite dall'Autorità Garante con il richiamato Provvedimento n. 55/2019 dandone evidenza nell'ambito dell'Informativa sul trattamento dei dati personali per l'erogazione di prestazioni sanitarie, anch'essa pubblicata sul proprio sito web aziendale www.asppalermo.org , alla Pagina "Privacy". (Allegato n°1)
- Qualora sia richiesto il consenso dell'interessato, lo stesso deve essere reso mediante sottoscrizione di apposita modulistica in uso presso le Unità Operative, previa visione e presa d'atto dell'Informativa.
- L'eventuale rifiuto a prestare il consenso al trattamento dei dati per finalità diverse da quelle di cura, comporta l'impossibilità di effettuare il relativo trattamento dei dati.
- Se il consenso dell'Interessato è prestato nel contesto di una dichiarazione scritta che riguarda 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.
- L'interessato **ha il diritto di revocare** il proprio consenso al trattamento dei dati personali in qualsiasi momento e ciò non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'Interessato è informato di ciò.
- La manifestazione del consenso sarà valida ed efficace fino alla revoca dello stesso.
- Il consenso è revocato con la stessa facilità con cui è accordato.

- Qualora il trattamento dei dati personali sia fondato sul rilascio del preventivo consenso da parte dell'Interessato, è compito della ASP - PA dimostrare che questi abbia prestato il proprio consenso libero e informato al trattamento dei dati personali.
- Il Titolare assicura attraverso idonee modalità l'archiviazione dei consensi espressi dagli interessati in modo da rendere fruibili e rintracciabili le autorizzazioni da questi rilasciate.
- **Il consenso al trattamento dei dati è comunque distinto dal consenso informato alla prestazione sanitaria.**

ART. 12 - REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

1. L'ASP - PA quale Titolare del trattamento redige, conserva ed aggiorna il Registro delle Attività di Trattamento svolte sotto la propria responsabilità. Esso viene predisposto per contenere la rilevazione dei trattamenti dei dati suddivisi per tipologie e per strutture organizzative, come presupposto necessario per adempiere agli obblighi di legge. Per ogni tipologia di trattamento sono indicate le informazioni di cui ai successivi commi 2 e 3.
2. Il registro contiene tutte le informazioni previste dall'art. 30 del Regolamento UE:
    - il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento, del Rappresentante del Titolare del trattamento e del Responsabile della Protezione dei Dati;
    - Denominazione e Descrizione del Trattamento;
    - Finalità del Trattamento;
    - Base Giuridica e Fonte Normativa;
    - Categorie di Interessati e Tipologia del Dato;
    - Trasferimento dei Dati in Paesi Terzi (Extra UE);
    - Termine di Conservazione dei Dati;
    - Trattamento Automatizzato;
    - Trattamento Cartaceo;
    - Destinatari dei Dati;
    - Responsabili del Trattamento;
    - Contitolari del Trattamento;
    - Trattamento su Larga Scala;
    - Misure di Sicurezza;
    - Informativa;
3. Il Registro dei Trattamenti è tenuto dalla U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali", in formato elettronico stampabile, e deve riportare la data della sua prima istituzione, unitamente alla data di eventuali aggiornamenti.
4. Il Registro dei Trattamenti viene aggiornato periodicamente in caso di modifiche ai trattamenti effettuati dalla ASP - PA. È compito dei singoli Delegati/Designati, sotto la propria responsabilità e nell'ambito dei trattamenti afferenti alla propria struttura, comunicare tempestivamente al Titolare, per il tramite della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali", casi di attivazione di nuovi trattamenti, modifiche o cessazioni di trattamenti in essere; nei casi di nuovo trattamento sarà cura del Titolare valutare la necessità di acquisire un preventivo parere in merito da parte del RPD.
5. Nel caso in cui la ASP – PA sia designata Responsabile del trattamento, deve tenere, altresì, un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare di riferimento. Tale Registro dovrà contenere:
    - il nome e i dati di contatto del Titolare del Trattamento di riferimento e, ove applicabile, del Responsabile della Protezione dei Dati;
    - le categorie dei trattamenti effettuati per conto del Titolare del Trattamento di riferimento;
    - 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 Regolamento UE, la documentazione delle garanzie adeguate;

- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento UE.

6. Su richiesta, la ASP - PA, in qualità di Titolare del trattamento o, ove applicabile, il Responsabile del trattamento, mettono il registro a disposizione dell'autorità di controllo.

ART. 13 – LIMITI ALLA CONSERVAZIONE DEI DATI PERSONALI

L'ASP di Palermo assicura l'adozione di apposite misure attraverso le quali:

- si proceda alla distruzione dei dati personali secondo le modalità previste dalla legge e una volta terminato il limite minimo di conservazione dei documenti analogici e digitali e dei dati personali ivi riportati;
- siano smaltiti gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è Titolare l'ASP - PA;
- il riutilizzo di apparati di memoria o hardware sia effettuato con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è Titolare l'ASP - PA..

DIRITTI DELL'INTERESSATO

ART. 14 - DIRITTO DI ACCESSO

Gli interessati possono contattare il Titolare del trattamento o in alternativa il Data Protection Officer R.P.D./D.P.O. per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.
Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 679/2016, 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:

- Le finalità del trattamento;
- Le categorie di dati personali in questione;
- 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;
- Quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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;
- Il diritto di proporre reclamo a un'autorità di controllo;
- Qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- L'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'accesso ai dati è garantito, all'Interessato, nei seguenti modi:

- Direttamente anche per via telematica se disponibile;
- Per il tramite del proprio medico di medicina generale;
- Per delega o procura.

ART.15 - DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 679/2016, 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.

ART. 16 - DIRITTO ALLA CANCELLAZIONE (Diritto all'Oblio)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 679/2016, in capo all'interessato è riconosciuto il "**diritto all'Oblio"**, che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata
L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- I dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti altrimenti trattati;
- L'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- L'interessato si oppone al trattamento in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano e non sussiste alcun motivo legittimo prevalente per procedere al trattamento oppure qualora i dati personali siano trattati per finalità di marketing diretto;
- I dati personali sono stati trattati illecitamente;

- I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- I dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 del Regolamento UE 2016/679.

ART. 17 - DIRITTO DI LIMITAZIONE DI TRATTAMENTO

Il diritto disciplinato dall'articolo n. 18 del Regolamento UE 2016/679 , è un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del Titolare).
Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).
Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, il Titolare può prevedere nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

ART. 18 - DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dall'articolo 20 del Regolamento UE 2016/679, che permette agli interessati di ricevere i dati personali forniti a un titolare, e trasmetterli senza impedimenti a un altro titolare del trattamento.
Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE).
Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'interessato, se tecnicamente possibile.

ART. 19 - DIRITTO DI OPPOSIZIONE

L'Interessato ha il diritto di opporsi (articolo 21 del Regolamento UE 2016/679) in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'Azienda si astiene dal trattarli ulteriormente, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici l'Interessato 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. 20 - COMUNICAZIONE DEI DATI PERSONALI ALL'ESTERNO

Secondo l'art. 44 del Regolamento UE 2016/679, la comunicazione dei dati personali all'esterno dell'ASP - PA è effettuata esclusivamente nei seguenti casi:

- a enti o aziende del SSN, della Pubblica Amministrazione e ad altri soggetti di natura pubblica eprivata, in esecuzione di obblighi derivanti da normative vigenti o per lo svolgimento delle funzioni istituzionali;
- qualora la comunicazione di dati personali ad altro soggetto pubblico non sia prevista da normativa vigente, verrà effettuata solo se prevista dal Regolamento per il Trattamento dei Dati Personali Sensibili e Giudiziari il cui schema tipo è stato approvato dal Garante, ovvero previa comunicazione alla stessa Autorità. La suindicata trasmissione dei dati personali avviene in forma cartacea o digitale.

RUOLI E RESPONSABILITÀ

ART. 21 - ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI MODELLO ORGANIZZATIVO PRIVACY

Nel presente capitolo sono riportate le figure dell'organizzazione privacy dell'ASP- PA coinvolte nell'applicazione della normativa sulla tutela dei dati personali nonché i compiti ad esse assegnati.

L'organigramma si sviluppa, in particolare, attraverso un sistema di governance articolato in tre tipologie di Ruoli:

- **RUOLI PRIVACY DEFINITI PER L'ESECUZIONE DEGLI ADEMPIMENTI**

- Visti il Regolsmento UE 2016/679, il D.Lgs. n.196/2003 così come modificato dal Decreto Legislativo n.101 del 10 agosto 2018 e considerata la vigente normativa, il modello organizzativo dell'ASP - PA per l'esecuzione degli adempimenti e dei trattamenti dei dati personali è costituito dalle seguenti figure
  - Il **Titolare del Trattamento** di seguito, per brevità, anche il "Titolare";
  - I **Soggetti Delegati/Designati** al Trattamento dei dati personali
  - I **Responsabili del Trattamento** dei dati personali
  - Le **Persone Autorizzate al Trattamento** di dati personali, di seguito per brevità, anche, gli "**Autorizzat**i";
  - Gli **Amministratori di Sistema** di seguito, per brevità, anche gli "AdS".

- **RUOLI PRIVACY PER LA SORVEGLIANZA E IL MONITORAGGIO SUGLI ADEMPIMENTI PRIVACY**

- Per la sorveglianza sull'osservanza degli adempimenti privacy in ambito aziendale la figura di riferimento è il **Responsabile della Protezione dei Dati** personali (di seguito per brevità "R.P.D./D.P.O.")..

- **RUOLI PRIVACY DI SUPPORTO PER LA GESTIONE DEGLI ADEMPIMENTI PRIVACY**

- L'Unità Operativa Semplice "Data Protection Officer e Sistema di Sicurezza nei Rapporti Istituzionali", è la struttura organizzativa che ha la missione di supportare il Titolare e il R.P.D./D.P.O. nella gestione degli adempimenti privacy dell'ASP – PA.

ART. 22 - TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati è l'Azienda Sanitaria Provinciale di Palermo,, con sede in Via Giacomo Cusmano n°24 – 90141 Palermo, persona giuridica di diritto pubblico, che esercita i poteri propri del Titolare del trattamento per mezzo del legale rappresentante pro-tempore Direttore Generale o Commissario Straordinario che singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Gli indirizzi di Posta Elettronica del Titolare sono i seguenti:
PEC: **direzionegenerale@pec.asppalermo.org**
EMAIL: direzionegenerale@asppalermo.org
Il Titolare dovrà mettere in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che i trattamenti posti in essere sono conformi al GDPR.
Il Titolare, avvalendosi della supervisione e collaborazione del Responsabile della Protezione dei Dati aziendale (R.P.D.) o detto anche Data Protection Officer (D:P:O.), provvede:

- a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale necessità di comunicazione;
- a individuare i Direttori/Responsabili delle strutture organizzative aziendali da nominare, con successivo atto, quali soggetti Delegati/Designati al Trattamento dei Dati Personali

impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione alle informazioni da rendere 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 previsti dagli artt. 15-22 del GDPR, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;

- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente alla vigente normativa di settore in materia di protezione dei dati personali oltre che al presente Regolamento.

Le responsabilità del Titolare del trattamento sono regolamentate, in termini generali, dall'Art. 24 del Regolamento UE 2016/679 con particolare riferimento ai seguenti punti:

- Tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento aziendale. Dette misure devono essere riesaminate e aggiornate qualora necessario.
- Le misure di cui sopra includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte della ASP - PA.
- Al fine di dimostrare il rispetto degli obblighi indicati dalla normativa vigente applicabile da parte del titolare del trattamento, può essere prevista l'adesione a codici di condotta di cui all'articolo 40 del Regolamento UE o a un meccanismo di certificazione di cui all'articolo 42 del Regolamento UE.

I compiti del Titolare del Trattamento sono indicati nei seguenti punti:

- Assicurare l'attuazione delle misure tecniche, giuridiche ed organizzative, ivi incluse le politiche in materia di protezione dei dati, adeguate per garantire ed essere in grado di dimostrare la sicurezza dei dati e l'osservanza del GDPR fin dalla progettazione "**Data Protection By Design**" e per impostazione predefinita "**Data Protection By Default**" di cui all'art. 25 del GDPR (Allegato n° 3);
- Procedere alla valutazione d'impatto privacy dei trattamenti - c.d. "data protection impact assessment" di seguito indicata con "**DPIA'** (art. 35 del Regolamento UE);
- Implementare un Sistema di Gestione della Protezione dei Dati, costituito da misure tecniche e organizzative adeguate, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR (art. 24, paragrafo 1 del Regolamento UE);
- Adottare "**Policy**" sul trattamento dei dati personali (art. 24, paragrafo 2 del Regolamento UE) o aderire a codici di condotta (art. 40) o conseguire certificazioni (art. 42 del Regolamento UE);
- Curare il rispetto dei principi applicabili al trattamento dei dati personali - c.d. "**Responsabilizzazione**" o "**Accountability**" - (art. 5, paragrafo 2 del Regolamento UE);
- Designare il Responsabile della Protezione dei Dati (c.d. R.P.D. o Data Protection Officer D.P.O. (art. 37, paragrafo 5 del Regolamento UE) e cooperare con lo stesso (art. 38, paragrafo 1 del Regolamento UE) sostenendolo nella sua attività (art. 38, paragrafo 2 del Regolamento UE) e garantendone indipendenza e autonomia (art. 38, paragrafo 3 del Regolamento UE);
- Nel caso di trattamenti effettuati per suo conto, provvede a designare i Responsabili del trattamento a norma dell'Art. 28 del RGPD che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate.
- Nel caso di esercizio associato di funzioni e servizi, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la Contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in

merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

- Curare, quando ne ricorrono le condizioni, la notifica di una violazione dei dati personali - c.d. "**Data Breach Notification**" all'Autorità Garante (art. 33 del Regolamento UE) e all'interessato (art. 34 del Regolamento UE);
- Rendere idonea informativa agli interessati (artt. 13 e 14 del Regolamento UE);
- Fornire idoneo e tempestivo riscontro alle richieste dell'interessato (art. 12, paragrafo 3 del Regolamento UE) nell'esercizio dei suoi diritti (artt. 15-22 del Regolamento UE);
- Redige, custodisce ed aggiorna, con il supporto del R.P.D./D.P.O., il Registro delle Attività di Trattamento effettuate sotto la propria responsabilità a norma dell'art. 30 del R.E. 2016/679;
- Cooperare con l'Autorità Garante (art. 31 del Regolamento UE), fornendogli ogni informazione necessaria (art. 58, paragrafo 1 del Regolamento UE);
- Effettuare periodicamente attività di verifica/**Audit**, atte a garantire il rispetto degli adempimenti normativi previsti dal GDPR avvalendosi del R.P.D./D:P:O.;
- Cooperare con gli organismi indipendenti di certificazione (art. 42, paragrafo 6 del Regolamento UE).

ART. 23 - CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 679/2016, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **Contitolari del Trattamento.** Essi determinano in modo trasparente, mediante un *accordo interno,* le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

ART.24 – GRUPPO DI LAVORO PRIVACY

In ossequio al principio dell'Accountability, l'ASP - PA ha ritenuto necessario identificare e costituire un nuovo Gruppo di lavoro che collabori con il Data Protection Officer nella gestione delle tematiche multidisciplinari, attinenti alla protezione dei dati, in coerenza con il Regolamento UE 679/2016.

Le complessità connesse alla natura multidimensionale e ai profili di responsabilità multilivello della materia, attinente alla protezione dei dati, richiedono la partecipazione attiva di un Gruppo di Lavoro composto da figure appartenenti alle diverse aree aziendali sia amministrative che sanitarie.

Ai fini della miglior attuazione dell'art. 39.b del Regolamento europeo 679/2016, l'attività di coordinamento è demandata al Data Protection Officer. I lavori del Gruppo si pongono i seguenti obiettivi:

- Partecipare attivamente al percorso progettuale in atto per acquisire competenze metodologiche e di dominio sul tema data protection;
- Abilitare canali di interazione interna al Gruppo di lavoro stesso ovvero rivolta ai soggetti aziendali con i quali confrontarsi in maniera continuativa e strutturata per rilevare le informazioni necessarie ai fini degli adempimenti normativi.

In ragione della preannunciata finalità, il Gruppo è composto da figure appartenenti alle diverse aree amministrative e sanitarie aziendali in base alle casistiche trattate e/o da trattare nonché potrà essere sempre integrato e/o modificato nella composizione.
Il R.P.D./D.P.O. sovraintende e verifica che le scelte assunte dal Gruppo siano poste in essere in ottemperanza a quanto previsto dalla normativa vigente.
Il Gruppo si riunisce ogni qual volta se ne presenti la necessità su convocazione del D.P.O .
In relazione agli argomenti da dibattere, le riunioni del Gruppo si svolgono in seduta ristretta o plenaria con la partecipazione di tutti i componenti. Delle riunioni del Gruppo si tiene verbale scritto.
Al fine di individuare e mettere in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità di trattamento, il R.P.D./D.P.O. potrà avvalersi, inoltre, dell'apporto di tutti gli ulteriori collaboratori aziendali che, in ragione della specifica professionalità, possano contribuire alla gestione delle attività del gruppo, che costituisce misura essenziale dell'accountability e del Sistema gestionale privacy dell'ASP – PA.

ART. 25 - DELEGATO/DESIGNATO ALLA GESTIONE DELLE ATTIVITA' DI TRATTAMENTO

L'art. 2-quaterdecies "Attribuzione di funzioni e compiti a soggetti designati" del Codice in materia di protezione dei dati personali, introdotto dal D.Lgs. 10 agosto 2018, n. 101 (v. art. 2, Modifiche alla parte I, titolo I, del decreto legislativo 30 giugno 2003, n. 196), ha introdotto la figura facoltativa del "Soggetto DESIGNATO/DELEGATO", prevedendo la possibilità di attribuire specifiche funzioni e compiti a soggetti Delegati/Designati dal Titolare o dal Responsabile.

L'ASP - PA, in qualità di Titolare del trattamento di dati personali, cioè quale soggetto che determina le finalità e i mezzi dei trattamenti dei dati effettuati nel proprio ambito, è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione delle responsabilità al fine di assicurare il rispetto delle disposizioni vigenti in materia, e ciò sulla base del principio europeo di "**Accountability**", che prevede il coinvolgimento e la responsabilizzazione, ad ogni livello, delle strutture dell'azienda nel percorso di adeguamento ai precetti europei.

Ciò detto, considerata la complessità dell'organizzazione dell'ASP – PA , in continuità con l'assetto organizzativo sin qui già progettato, Il Titolare provvede alla nomina dei Soggetti Delegati/Designatii che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia al Trattamento dei Dati Personali, individuandoli tra coloro che ricoprono gli incarichi di:

- Direttore Amministrativo Aziendale pro-tempore, per i trattamenti afferenti agli uffici della segreteria di propria competenza;
- Direttore Sanitario Aziendale pro-tempore, per i trattamenti afferenti agli uffici della segreteria di propria competenza;
- Direttore di Dipartimento Strutturale e Funzionale;
- Direttore delle Unità Operative Complesse, dell'area Amministrativa, Sanitaria, Tecnica e Professionale;
- Direttore di Distretto Sanitario;
- Direttore di Presidio Ospedaliero;
- Responsabili delle Unità Operative Semplici Dipartimentali;
- Responsabili delle Unità Operative Semplici. in Staff;
- Amministratore di Sistema.

La designazione di Delegato/Designeto è legata al conferimento dell'incarico di responsabilità della struttura o funzione e comporta lo svolgimento di attività di supporto al Titolare nel controllo, nella supervisione e nell'attuazione delle istruzioni e delle **Policy** aziendali.

I Delegati/Designati per l'esercizio dei compiti e delle funzioni affidate hanno il dovere di osservare la delega e a fare osservare le precauzioni e le disposizioni individuate dal Titolare in tema di sicurezza dei dati personali. Di seguito, a titolo esemplificativo, sono riportate le principali funzioni ed i compiti più rilevanti attribuiti ai Soggetti Designati:

- Comunica ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE riguardanti l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio;
- Comunica eventuali variazioni da apportare al Registro dei Trattamenti;
- Utilizza – per competenza - il modello aziendale di Informativa e Consenso e quelli eventualmente successivamente approvati dal Titolare, verificandone il rispetto;
- Collabora nella gestione delle istanze degli interessati;
- Contribuisce a far sì che tutte le misure di sicurezza riguardanti i dati dell'ASP - PA siano applicate all'interno dell'Azienda stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
- Mantiene aggiornato, per la struttura di propria competenza, il "Registro delle Attività di Trattamento" di cui all'art. 30 del GDPR, cooperando con il Titolare, con il R.P.D./D.P.O. e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4 del GDPR;
- Nomina e coordina " Autorizzati al trattamenti dei dati", fornendo le istruzioni necessarie, tutto il personale dipendente e non dipendente (es. tirocinanti, volontari, borsisti) che prestano servizio, anche temporaneamente, all'interno della struttura che il Delegato dirige e accedono ai dati personali di cui l'ASP - PA è Titolare.
- Assiste e coadiuva il Titolare nell'esecuzione degli adempimenti previsti dalla vigente normativa privacy. Per tale funzione può essere dotato di specifiche autonomie decisionali circa le modalità del trattamento;
- Garantisce il rispetto degli adempimenti privacy per le attività istituzionali dell'ASP - PA affidate alla propria Struttura/Area e che implicano un trattamento di dati personali;
- Garantisce che la raccolta dei dati personali e le operazioni di trattamento affidate alla propria Struttura/Area, avvengano per scopi determinati, espliciti e legittimi e che i dati trattati siano esatti, pertinenti, completi, non eccedenti e conservati per un periodo non superiore a quello necessario per gli scopi del trattamento;
- Segnala, alla U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" e al R.P.D./D.P.O., eventuali specifici interventi formativi in tema di privacy per il personale della struttura di propria competenza da prevedere nell'ambito del piano dei fabbisogni formativi;
- Adotta, nell'ambito delle specifiche funzioni di attuazione assegnate dal Titolare, le misure tecniche e organizzative per la protezione e la sicurezza dei dati;
- Individua quali Responsabili del trattamento ex art. 28 del GDPR, i soggetti esterni cui ASP – PA affida servizi che implicano un trattamento di dati personali e che rientrano nella titolarità dell'Azienda comunicando al Titolare ed al R.P.D./D.P.O. i riferimenti contrattuali relativi all'atto deliberativo e gli aggiornamenti in merito al fine di provvedere, prima dell'inizio delle attività di trattamento, alla designazioni dei suddetti quali Responsabili del trattamento dei dati;
- Coinvolge il R.P.D./D.P.O. in tutte le questioni inerenti la protezione dei dati personali nelle situazioni previste dalle leggi e nell'ambito dei processi aziendali;
- Informa il Titolare del trattamento ed il R.P.D./D.P.O., senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali (cd. **data breach**) nel rispetto delle tempistiche e delle modalità previste e assistere il Titolare nelle comunicazioni all'interessato di cui all'art. 34 GDPR;
- Collabora nelle verifiche interne per la sorveglianza in tema di privacy, fornendo le informazioni e i documenti richiesti;

- Mette a disposizione del Titolare, su richiesta scritta di quest'ultimo, tutte le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dall'atto della sua nomina.
- Consente al Titolare e al R.P.D./DPO di eseguire verifiche e ispezioni (congiuntamente "**Audit**") sulle informazioni di cui al comma precedente, e si impegna ad assistere il Titolare, al fine di dimostrare, con riferimento al trattamento di dati svolto per compiti istituzionali, l'adempimento degli obblighi previsti dall'atto della sua nomina. Gli Audit potranno anche essere condotti direttamente da personale del Titolare o da un revisore terzo indipendente da esso incaricato.
- Ottempera ad ogni altro adempimento stabilito dal Titolare in relazione al trattamento dei dati personali.

I compiti affidati al Soggetto Delegato/Designato, così come l'ambito organizzativo di competenza, sono analiticamente specificati per iscritto dal Titolare nell'atto di nomina di designazione in conformità a quanto disposto dall'art. 2 – quaterdecies del D.Lgs. 196/2003 e ss.mm.ii.
Ulteriori dettagli circa i compiti assegnati ai Soggetti Delegati/Designati sono specificati nei relativi atti di designazione.

Per la nomina dei Soggetti Delegati/Designati, sopra indicati, deve essere utilizzato il modello di nomina predisposto dall'ASP – PA (**Allegato n° 3**) salvo adattarli alle specifiche esigenze delle funzioni e strutture organizzative presso cui i Soggetti Designati eseguiranno i trattamenti.

Il Titolare del trattamento può, con successivo atto, individuare quali Delegati/Designati al trattamento anche altri soggetti (dirigenti/responsabili di Struttura/area), oltre a quelli previsti dal presente Regolamento, in virtù delle modifiche dell'atto aziendale, delle particolarità organizzative e funzionali delle attività di competenza e in virtù di nuove assunzioni al ruolo di dirigente/responsabile di Struttura/Area.

ART. 25.1 - DELEGATI/DESIGNATI DI AREA TECNICO -AMMINISTRATIVA
I responsabili di struttura quali "Delegati/Designati" di Area Tecnico-Amministrativa", ai sensi dell'articolo 2-quaterdecies Codice Privacy, che provvedono alla definizione di atti aventi natura negoziale (Contratti/Convenzioni, ecc.), qualora in tali **contratti e/o convenzioni** risultino Trattamenti di Dati Personali in nome e per conto del Titolare del Trattamento, da parte dei fornitori stessi, al fine di poterli nominare Responsabili del Trattamento, ai sensi dell'art. 28 del GDPR, in aggiunta ai compiti e alle funzioni di cui al punto 4.3:

- Provvedono in fase preliminare alla definizione di contratti e/o convenzioni, con l'ausilio della U.O.S. "Data Protection Officer e Sistemi Informatici nei Rapporti Istituzionali" ed eventuale consultazione del R.P.D./D:P:O., alla valutazione dei fornitori in merito al possesso di garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento dei dati soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;
- Individuano i soggetti esterni o società cui ASP – PA affida servizi che implicano necessariamente un trattamento di dati personali e che rientrano nella titolarità dell'Azienda e comunicano al Titolare ed al Responsabile della U.O.S. "Data Protection Officer e Sistemi Informatici nei Rapporti Istituzionali" i riferimenti contrattuali relativi all'atto deliberativo e gli aggiornamenti in merito al fine di consentire al Titolare, prima dell'inizio delle attività di trattamento, la sottoscrizione del relativo atto di nomina a Responsabili del trattamento, ai sensi dell'art. 28 del GDPR.

La U.O.S. "Data Protection Officer e Sistemi Informatici nei Rapporti Istituzionali" avrà, anche, il compito della tenuta dell'elenco aggiornato di tutti i contratti di nomina ex art. 28 GDPR sottoscritti dall'entrata in vigore del GDPR.

ART. 26 - AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Per persona Autorizzata al trattamento dei Dati Personali si intende il personale dell'ASP – PA che nell'espletamento delle proprie mansioni esegue materialmente le attività che implicano un trattamento di dati personali e che hanno ricevuto formale lettera di nomina in conformità agli artt. 28 paragrafo 3, lett. b), 29 e 32 paragrafo 4 del Regolamento UE 2016/679 (GDPR) e dell'art. 2-quaterdecies del D.Lgs. 196/2003 così come integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101.

Gli Autorizzati devono garantire il rispetto degli adempimenti privacy nell'esecuzione delle attività ad esse assegnate. All'Autorizzato sono affidati compiti di riservatezza e osservanza di regole di sicurezza rispetto ai trattamenti che effettua, con obbligo di attenersi alle istruzioni ricevute.

Gli Autorizzati, nell'ambito della struttura aziendale di appartenenza, ricevono da parte del soggetto Delegatio/Designato del trattamento un atto formale di nomina individuale, che impartisce loro disposizioni sul corretto uso dei dati, in special modo sotto il profilo della sicurezza, e vengono informati sulle direttive vigenti sulla protezione dei dati da loro trattati. **L'atto di designazione costituisce l'unico presupposto di liceità per il trattamento dei dati personali**, dovrà essere controfirmato per accettazione dallo stesso Autorizzato, e custodito a cura del Delegato/Designato della struttura di appartenenza.

Il Delegato/Designato istruisce gli Autorizzati al Trattamento dei Dati assicurandosi, attraverso le attività di monitoraggio previste nei processi aziendali, che forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento.

Le responsabilità per una corretta gestione dei dati ed i compiti affidati all'Autorizzato, così come l'ambito dei trattamenti di competenza sono specificati per iscritto dal Delegato/Designato e riportati nell'atto di nomina.

Ai fini della nomina di ciascuno Autorizzato al Trattamento, i Delegati/Designati devono avvalersi dei modelli di nomina predisposti dall'ASP – PA (**Allegato n° 4**) e, ove necessario, adattarli alle specifiche esigenze delle attività svolte nelle strutture organizzative di appartenenza all'interno delle quali verranno eseguiti i trattamenti.

Viene stabilito, inoltre, che l'atto formale di nomina quale soggetto Autorizzato al Trattamento non seguirà il dipendente e si intenderà revocato di diritto in caso di risoluzione del rapporto di lavoro e/o di nuovo incarico o trasferimento presso altra Struttura aziendale dove sarà necessario formalizzare un nuovo atto di nomina.

Di seguito, a titolo esemplificativo, sono riportati alcuni dei principali compiti e degli obblighi previsti più rilevanti in capo agli Autorizzati:

- Raccogliere i dati personali e successivamente trattarli per il solo perseguimento delle finalità istituzionali dell'ASP - PA e, comunque, per scopi determinati, espliciti e legittimi. I dati devono essere esatti, pertinenti, completi, non eccedenti e conservati per un periodo non superiore a quello necessario per gli scopi del trattamento;
- Trattare i dati, sia in modalità informatica e telematica, sia cartacea, osservando le modalità operative impartite dall'ASP – PA, anche con riferimento agli aspetti relativi alla sicurezza;
- Coadiuvare il Soggetto Delegato/Designato nelle attività inerenti all'esercizio dei diritti dell'interessato;
- Il Soggetto Autorizzato qualora tratti dati con l'ausilio di strumenti informatici è personalmente responsabili della gestione riservata della password assegnata, ed è fatto assoluto divieto di cedere la propria password ad altri;

- Il Soggetto Autorizzato è responsabile della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento e hanno l'obbligo di restituirli al termine delle operazioni affidate.
- Il Soggetto Autorizzato può trattare i dati personali nella misura necessaria a raggiungere gliobiettivi relativi alle attività istituzionali svolte dall'Unità Operativa di appartenenza. Le attività ditrattamento di dati personali sono correlate allo svolgimento delle proprie funzioni.
- Il Soggetto Autorizzato dovrà effettuare il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare e/o dal Soggetto Delegato/Designato in forma scritta. L'atto di nomina costituisce parte delle istruzioni del Titolare e/o del Delegato/Designato per il trattamento dei dati personali da parte del Soggetto Autorizzato e potrà essere integrato, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte delTitolare e/o del Delegato/Designato..
- Il soggetto Autorizzato si impegna a mantenere la riservatezza dei dati trattati e si assoggetta a tale obbligo.
- Il soggetto Autorizzato si impegna ad adottare le misure richieste dall'Art. 32 del GDPR secondo le istruzioni impartite
- Il Soggetto Autorizzato si impegna ad Informare, tempestivamente e senza ingiustificato ritardo, il Titolare e/o per suo conto il Soggetto Delegato/Designato e il RPD/DPO, di ogni violazione di dati personali (cd**. Personal data breach**) nel rispetto delle tempistiche e delle modalità indicate nell'atto di nomina.

Tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito delle strutture del Titolare, pur non essendo dipendenti o titolari di incarichi conferiti dall'ASP – PA (es.: consulenti, tirocinanti, borsisti, collaboratori in genere), devono essere nominati formalmente dal Delegato/Designato della struutura presso la quale espletano servizio soggetti Autorizzati al trattamento dei dati personali.

Ulteriori dettagli relativi alla designazione dei Soggetti Autorizzati al Trattamento sono specificati nel modello di nomina allegato al presente Regolamento.

ART. 27 - PERSONA FISICA ESTERNA ALLA STRUTTURA DEL TITOLARE AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI

Tutto il personale non dipendente dell'ASP - PA che presta comunque attività all'interno dell'Azienda stessa a qualsiasi titolo (es.: personale addetto alle pulizie), con o senza retribuzione, qualora in ragione della propria attività venga a conoscenza di dati personali trattati dall'Azienda o possa accedere ai locali di trattamento dati è tenuto al rispetto del presente Regolamento e, in particolare:

- Deve mantenere la massima riservatezza sulle notizie e le informazioni di cui venga conoscenza;
- Deve astenersi dall'effettuare operazioni di trattamento dei dati salvo che non sia individuato quale Soggetto Autorizzato al trattamento dei dati.

ART. 28 - RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

Il Responsabile del Trattamento ai sensi dell'art. 28 del GDPR è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, in virtù di apposito contratto di servizio o altro atto scritto equivalente, tratta i Dati Personali per conto del Titolare.

L'ASP – PA disciplina le attività di trattamento dei dati personali affidate ai soggetti esterni con un apposito "Atto di nomina a Responsabile", ai sensi dell'art. 28 del Regolamento UE 2016/679, sottoscritto, con firma digitale, nella persona del legale rappresentante pro-tempore dell'ASP –PA, in qualità del Direttore Generale o Commissario Straordinario e controfirmato digitalmente per accettazione da parte del Legale Rappresentante pro-tempore del Responsabile del trattamento.

La sottoscrizione per accettazione dell' atto di nomina vincola il Responsabile e l'eventuale Sub-Responsabile al Titolare del trattamento dei dati personali, in particolar modo per quanto riguarda la durata, la natura e la finalità del trattamento, il tipo di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.
L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.
Ai sensi dell'art. 28 del Regolamento UE, qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo deve ricorrere unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato
I Responsabili sono principalmente riconducibili alla categoria dei fornitori di beni e/o servizi che trattano dati personali per conto del Titolare del trattamento. A tal proposito la ASP – PA designa Responsabili del Trattamento dei Dati Personali tutti i soggetti esterni cui sono affidate attività di competenza aziendale o attività connesse strumentali e di supporto, ivi incluse le attività manutentive che comunque comportano necessariamente il trattamento di dati personali.

Ai fini del presente Regolamento privacy, il contratto o altro atto giuridico che ne disciplina gli obblighi prevede, in particolare, che il responsabile del trattamento debba:

- Trattare i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro, alla Convenzione, alla Delibera di nomina/aggiudicazione e al Contratto Principale. I servizi che potranno essere svolti dal Responsabile sono indicati nei documenti sopra richiamati e, eventualmente, in altri documenti prodotti dal Titolare.
- La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile deve corrispondere alla durata indicata nel contratto. Nel caso in cui, nell'ambito del trattamento svolto per conto del Titolare, il Responsabile fosse tenuto a conservare dati personali, la durata della conservazione dovrà essere pari alla durata contrattuale se non previsto diversamente da specifica disposizione di legge o, nei casi previsti dalla legge, di regolamento o in generale a livello normativo.
- I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi dell'atto di designazione sono, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori del Titolare, terzi incaricati, a qualunque titolo, dal Titolare, pazienti, controparti contrattuali del Titolare e, in generale, terze parti rispetto alle quali l'ASP – PA agisce come Titolare del trattamento dei dati personali ai sensi del Regolamento UE 2016/679. I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute
- Il Responsabile dovrà effettuare il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite dovrà essere indicato nello specifico allegato all'atto di designazione. L'atto di designazione e il Contratto Principale costituiscono parte delle istruzioni dell'ASP - PA per il trattamento dei dati personali da parte del Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare. Tali istruzioni dovranno essere fornite dal Titolare anche in caso di necessità di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il Responsabile del trattamento dovrà informare il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
- Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nel Contratto e nell'Atto di Nomina dovrà essere trasmessa dall'ASP - PA al Responsabile per iscritto e comunicata

via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

- Il Responsabile dovrà garantire che i soggetti da lui autorizzati al trattamento dei dati personali si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.
- Il Responsabile dovrà impegnarsi ad adottare le misure richieste dall'art. 32 del GDPR.
  In particolare, in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile dovrà impegnarsi a mettere in atto le misure tecniche e organizzative adeguate, indicate negli allegati all'atto di designazione di cui si dovrà richiedere la compilazione per la descrizione delle modalità di implementazione. Il Responsabile dovrà impegnarsi a comunicare le indicazioni applicabili ai prodotti e/o servizi forniti secondo quanto previsto dall'Atto di designazione (tale obbligo vige solo per i Responsabili fornitori di servizi tecnici/tecnologici o per specifici requisiti).
- Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Atto di designazione, in considerazione del progresso e sviluppo tecnologico, dovrà effettuare una preventiva comunicazione all'ASP – PA quale Titolare, fermo restando che tali modifiche non dovranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Atto di designazione.
- Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nel Contratto, il Responsabile dovrà impegnarsi ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli artt. da 15 a 22 del Regolamento UE.
- Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli artt. da 15 a 22 del regolamento UE nell'ambito delle attività di trattamento di dati personali svolti per conto del Titolare.
- Tenendo conto della natura del trattamento, come descritto nel Contratto e nell'atto di designazione, e delle informazioni di volta in volta messe a disposizione, il Responsabile dovrà impegnarsi ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del Regolamento UE.
- I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dal Contratto e nell'atto di designazione, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, dovranno essere periodicamente cancellati ove ne ricorra il termine in base a quanto previsto. Alla cessazione del Contratto, i dati oggetto di Trattamento da parte del Responsabile dovranno essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali, salvo che la legge applicabile (diritto dell'Unione o degli Stati membri) obblighi il Responsabile alla conservazione dei dati personali trattati.
- Informare il Titolare del trattamento e il R.P.D./D.P.O senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza (cd. **Personal Data Breach**) che comporti accidentalmente o in modo illecito la distruzione, la perdita la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.
- Oltre a quanto già previsto dal precedente comma, il Responsabile dovrà, ai sensi dell'art. 28.3, lett. f) del Regolamento UE 2016/679, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del Regolamento UE 2016/679 o di

comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR. Secondo quanto previsto dalla Procedura di Gestione delle Violazioni di Dati Personali, allegata al presente Regolamento, la comunicazione delle suddette violazioni dovrà avvenire a mezzo PEC/mail rispettivamente ai seguenti indirizzi: direzionegenerale@pec.asppalermo.org e rpd@pec.asppalermo.org .

- Inoltre, il Responsabile dovrà fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della "**Valutazione di Impatto"** sulla protezione dei dati, "**Data Protection Impact Assessment**", di seguito per brevità "**DPIA**", qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento UE, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento UE.
- Fatta salva la possibilità di nominare un Sub - Responsabile, il Responsabile deve garantire che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi oggetto del Contratto.
- Il Responsabile deve impegnarsi a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali dell'ASP - PA, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività svolte per conto dell'ASP - PA, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.
- Il Responsabile, su richiesta del Titolare, dovrà coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.
- Il Responsabile dovrà mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare contenute nell'atto di designazione e dovrà consentire al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.
- Il Titolare dovrà dare comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.
- Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile dovrà impegnarsi altresì a:

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

- Qualora il Responsabile (o eventuali suoi Sub-Responsabili) determini autonomamente le finalità e i mezzi di trattamento, in violazione delle istruzioni impartite dal Titolare, in base a quanto previsto dall'art. 28.10 del Regolamento UE 2016/679, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.
- La designazione in qualità di Responsabile non dovrà comportare alcun diritto per questi ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto stipulato con il Titolare.
- Il Responsabile dovrà tenere ed aggiornare costantemente il Registro dei Trattamenti svolti per conto dell'ASP - PA, secondo quanto previsto dall'art. 30.2 del Regolamento UE 2016/679.
- Il Titolare dovrà poter chiedere copia del Registro dei Trattamenti del Responsabile per i trattamenti svolti per conto dell'ASP - PA e copia della documentazione relativa agli adempimenti privacy attuati dal Responsabile nell'ambito del servizio svolto per conto del Titolare.
- Eventuali modifiche e/o integrazioni all'atto di designazione del Responsabile, previamente concordate con il Titolare, dovranno essere poste in atto in uno specifico articolo dell'atto stesso denominato"Accordi Specifici".

Ulteriori dettagli relativi alla designazione dei Responsabili del Trattamento sono specificati nel modello aziendale dell'Atto di nomina a Responsabile, ai sensi dell'art.28 del Regolamento UE 2016/679,. predisposto dall'ASP – PA, da utilizzare, adattare, personalizzare, in base alle specifiche situazioni. (**Allegato n°5**)

ART. 29 – SUB RESPONSABILI DEL TRATTAMENTO

1. Per l'esecuzione di specifiche attività per conto dell'ASP - PA, il Responsabile potrà avvalersi di "Sub–Responsabili" del trattamento ai sensi del Regolamento UE 2016/679. I Sub - Responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-responsabili del Trattamento, essi dovranno essere vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nell'accordo di designazione tra l'ASP – PA quale Titolare del trattamento e il Responsabile, prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 2016/679. Secondo quanto previsto dall'art. 28.4 del Regolamento UE, qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserverà nei confronti dell'ASP - PA quale Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile.
2. L'accordo di designazione tra il Responsabile ed il Sub-Responsabile dovrà essere fornito in copia al Titolare in maniera che esso possa verificarne la conformità rispetto ai requisiti definiti per il Responsabile; tale accordo potrà essere anche pre-esistente all'accordo di designazione del Responsabile del Trattamento da parte del Titolare. Nell'accordo di designazione tra il Responsabile ed il Sub - Responsabile, dovrà essere previsto un ruolo di Sub-Responsabilità da parte del Sub-Responsabile.
3. L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto e all'Atto di Designazione dovrà essere previamente fornito al Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco. Alla richiesta di autorizzazione da parte del Responsabile, dovrà essere allegato l'accordo di designazione del Sub-responsabile.

4. Il Responsabile si impegna a informare anticipatamente il Titolare, tramite PEC, laddove intenda:
   - includere un nuovo Sub-Responsabile del Trattamento nell'elenco,
   - sostituire o cessare il rapporto con un Sub-Responsabile del Trattamento esistente.

   La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 30 giorni dalla ricezione della comunicazione da parte del Responsabile
5. Qualora il Titolare sollevi obiezioni su uno o più Sub-Responsabili del Trattamento, il Titolare dovrà dare indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà: proporre altro Sub-Responsabile del Trattamento in sostituzione del Sub-Responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; oppure adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
6. Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-Responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.
7. Ulteriori dettagli relativi alla designazione dei Sub-Responsabili del Trattamento sono specificati nello specifico modello di nomina utilizzato dall'ASP- PA, allegato al presente Regolamento. Dopo l'approvazione, il presente Regolamento verrà trasmesso a tutte le strutture aziendali interessate, evidenziando la necessità di provvedere alle nomine dei Responsabili utilizzando l'apposita modulistica aziendale (Allegato n°6). L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

ART. 30 - RESPONSABILE DELLA PROTEZIONE DEI DATI

L'ASP – PA ha provveduto al conferimento dell'incarico di Responsabile della Protezione dei Dati "R.P.D." (in lingua inglese Data Protection Officer – D.P.O.) con con atto di nomina del Commissario dell'ASP - PA, prot. n° ASP/8635/2018 del 19 febbraio 2018, ricorrendo ad una figura interna, scelta in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e che svolge principalmente funzioni di informazione, consultazione, controllo, sorveglianza dell'osservanza del GDPR, in conformità a quanto disposto dagli artt. 37, 38 e 39 del GDPR e delle Linee Guida del Garante sui Responsabili della protezione dei dati del 14 Luglio 2017.

L'ASP – PA quale Titolare del trattamento, secondo quanto previsto dagli artt. 37 e 38 del GDPR, garantisce al R.P.D./D.P.O. autonomia funzionale, autonomia finanziaria, conoscenza dei processi interni aziendali, aggiornamento continuo in materia di protezione dati personali, per lo svolgimento delle proprie funzioni.

Ai fini del presente Regolamento privacy, il R.P.D./D.P.O. dell'ASP - PA, come risulta dalle previsioni del GDPR , ha il compito di:

- Sorvegliare l'osservanza del GDPR, del D.Lgs. 196/2003 e ss.mm.ii., di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati, nonché alle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento;
- Informare e fornire consulenza al Titolare del Trattamento, nonché ai Soggetti Delegati/Designati, alle Persone Autorizzate in merito all'esecuzione dei trattamenti e agli obblighi derivanti dal Regolamento UE 2016/679 e da altre disposizioni dell'Unione relative alla protezione dei dati;

- Fornire pareri al Delegato/Designato per l'individuazione di soggettività e ruoli, nell'ambito dei rapporti Istituzionali, e dei soggetti che effettuano il Trattamento dei Dati.
- Validare le Informative aziendali ex Artt.13 e 14 del Regolamento UE 2016/679 redatte dalla U.O.S. "Data Protection Officer e Sistemi di Sicurezzaa nei Rapporti Istituzionali";
- Individuare e predisporre le proposte formative del Piano Formazione Annuale Aziendale, in collaborazione con il responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezzaa nei Rapporti Istituzionali" e con il Delegato/Designato di Struttura;
- Redigere un parere valutativo sui trattamenti in base alla "Procedura di applicazione del **Principio di Privacy by Design e Privacy by Default**" - su indicazione del Delegato/Designato;;
- Redigere un parere sulla necessità di presentare un esposto o di sporgere denuncia, anche contro ignoti, all'Autorità Giudiziaria, in caso di attività penalmente rilevanti, quali attacchi cibernetici, sospetta attività fraudolenta o altri casi di sospetto illecito su indicazione del Delegato/Designato;
- Coordinare la effettuazione di "**Audit"** di verifica nelle strutture organizzative dell'ASP – PA quale Titolare del Trattamento e, se richiesto dallo stesso, presso i Responsabili di Trattamento.
- Supportare il Titolare ai fini del mantenimento e dell'aggiornamento del Registro delle attività di trattamento, collaborando con le pertinenti strutture aziendali per la gestione del suddetto Registro.
- Supportare il Titolare del Trattamento per tutte le attività relative alla notificazione/comunicazione di una violazione dei dati personali all'Autorità Garante e agli Interessati, di cui rispettivamente agli artt. 33 e 34 del GDPR, nel rispetto della documentazione dell'ASP – PA in materia di **Personal Data Breach**;
- Riferire del proprio operato al Titolare;
- Fornire, se richiesto, un parere al Titolare del Trattamento in merito alla valutazione d'impatto sulla protezione dei dati personali (cosiddetta "**Data Protection Impact Assessment**", di seguito per brevità "**DPIA**"), di cui all'art. 35 del GDPR e sorvegliarne lo svolgimento ai sensi dell'art. 39 p.1 lett. c) GDPR;
- Cooperare e fungere da punto di contatto con l'Autorità Garante Privacy per tutte le questioni connesse al trattamento dei dati tra cui la consultazione preventiva di cui all'art. 36 GDPR ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione (art. 39 p.1 lettera e) GDPR);
- Fungere da punto di contatto per gli interessati per tutte le questioni relative al trattamento dei dati personali e all'esercizio dei loro diritti previsti dal Regolamento e supportare il Titolare, i Soggetti Designati/Delegati e le Persone Autorizzate nei procedimenti ad essi correlati;
- Svolgere le funzioni comunque assegnate dalla normativa nel tempo di vigenza contrattuale.

Il R.P.D./R.P.O. opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento nè sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il R.P.D./D.P.O. non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.
Fermo restando l'indipendenza nello svolgimento di dette attività, il R.P.D./D.P.O. riferisce direttamente al Titolare o suo Delegato/Designato o al Responsabile del trattamento. Nel caso in cui siano rilevate dal R.P.D./D.P.O. o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso R.P.D./D.P.O., quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.
Con specifico riferimento agli obblighi posti in capo al Titolare nei confronti del R.P.D./D.P.O. rileva evidenziare che ai sensi dell'art. 38 c. 1 del GDPR "Il Titolare e il Responsabile del trattamento si assicurano che il Responsabile della Protezione dei Dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

ART. 31 - FUNZIONE PRIVACY DI SUPPORTO PER LA GESTIONE DEGLI ADEMPIMENTI PRIVACY

L' Unità Operativa Semplice "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" è la struttura organizzativa che ha la missione di supportare tutti i Soggetti Delegati/Designati e per il loro tramite il Titolare nella gestione degli adempimenti previsti dalla vigente normativa privacy.

Si riportano, a titolo esemplificativo e non esaustivo, i compiti più rilevanti di competenza:

- Ricezione ed acquisizione delle comunicazioni inviate dai Delegati/Designati di Struttura dell'ASP - PA relative all'avvio di un nuovo trattamento e/o a modifiche da apportare ai trattamenti già in corso;
- Analisi di ogni nuovo trattamento e/o della modifica dei trattamenti già in corso, comunicati dai Delegati/Designati di Struttura, e, se del caso, sentito il R.P.D./D.P.O., con conseguente integrazione e/o modifica del Registro del Trattamento dei Dati;
- Predisposizione, su indicazione della Direzione Aziendale, di accordi di Contitolarità, ai sensi dell'art.26 GDPR, sentito il R.P.D./D.P.O. con conseguente integrazione e/o modifica del Registro dei Trattamenti;
- Supporto ai Delegati/Designati di Area Tecnico-Amministrativa per la predisposizione delle bozze di accordi di nomina a Responsabile del Trattamento, di cui all'articolo 28 GDPR;
- Predisporre ex novo e/o di aggiornare le Informative di cui agli articoli 13 e 14 GDPR. previa validazione resa per iscritto dal R.P.D./D.P.O.. Le Informative redatte sono sia Pubblicate sul sito web dell'ASP – PA consultabile all'indirizzo www.asppalermo.org alla pagina privacy, che inviate al Delegato/Designato di Struttura affinché vengano fornite all'interessato rispettivamente al momento della raccolta dei Dati Personali, con riferimento all'Informativa ex articolo 13 del GDPR;
- Coordinamento del processo di notifica delle violazioni di Dati Personali come previsto dalla "Procedura operativa di gestione e notifica violazioni di dati personali (**Data Breach**)", previa intesa con il R.P.D./D.P.O. quale unico soggetto preposto ai rapporti con il Garante della Protezione dei Dati Personali ai fini della notifica e collaborazione con il Responsabile del servizio Informatico aziendale per le notifiche alle eventuali ulteriori autorità competenti (es. AGID e CSIRT);
- Valutazione dei nuovi trattamenti di Dati Personali e di quelli già svolti cui sono apportate modifiche sostanziali relativamente alla necessità di svolgimento della valutazione d'impatto sul Trattamento di Dati – **DPIA** – ai sensi dell'articolo 35 GDPR e secondo i parametri indicati nelle "Linee guida metodologiche per la conduzione del Risk Assessment e del Data Protection Impact Assessment (**DPIA**)".
- Ove risultasse necessario eseguire la "**DPIA"**, procede a supportare il R.P.D./D.P.O. aziendale,con la partecipazione del Delegato/Designato di Struttura coinvolto nel flusso in esame nonché dal Respomsabile del Servizio Informatico aziendaole (ove necessario) alla redazione della stessa.
- Valutazione della necessità di effettuazione della procedura di consultazione preventiva di cui all'articolo 36 GDPR e, ove necessario, svolgimento della stessa previo ottenimento del parere positivo, in forma scritta, del R.P.D./D.P.O.
- Segnalazione alla Direzione Generale, della necessità di presentare un esposto o di sporgere denuncia, anche contro ignoti, all'Autorità Giudiziaria in caso di attività penalmente rilevanti, quali attacchi cibernetici, sospetta attività fraudolenta o altri casi di sospetto illecito, con acquisizione del parere del R.P.D./D.P.O.
- Valutazione e gestione delle istanze presentate dagli interessati per l'esercizio dei diritti di cui agli articoli da 15 a 22 GDPR, con il supporto del R.P.D./ D.P.O. e del Delegato/Designato della Struttura aziendale di competenza..
- Individuazione e predisposizione delle proposte formative del Piano Formazione Annuale Aziendale, in collaborazione con il R.P.D./D.P.O., sulla base dei fabbisogni formativi in

materia di trattamento dei Dati dei soggetti Autorizzati al Trattamento rilevati dai Delegati/ Designati di Struttura e censiti dall'U.O.S. Formazione;

- Ove necessario, avviamento della procedura valutativa di cui alla "Procedura di applicazione del **Principio di Privacy by Design e Privacy by Default**" con la partecipazione del Delegato/ Designato di Struttura coinvolto nel flusso di trattamento esaminato, nonché del Responsabile del Servizio Informatico aziendale (ove necessario) e acquisizione obbligatoria del parere positivo, in forma scritta, del R.P.D./D.P.O..
- Collaborare e coordinarsi con il R.P.D./D.P.O. per le attività di sorveglianza e di monitoraggio sugli adempimenti privacy.

ART. 32 - AMMINISTRATORE DI SISTEMA

L'ASP – PA o il Responsabile del trattamento nomina un "Amministratore di Sistema" (o amministratore di rete), preposto a compiti di vigilanza e controllo sul corretto utilizzo del sistema informatico gestito e utilizzato.

Lo stesso viene individuato tra i dipendenti aziendali previa valutazione dell'esperienza, capacità e affidabilità, in grado di fornire idonea garanzia del rispetto delle vigenti disposizioni in ambito di trattamento dei dati e di sicurezza.

L'individuazione è da ritenersi personale e la designazione avviene con apposito atto di nomina sottoscritta dal Titolare del Trattamento, nella persona del Legale Rappresentante pro-tempore, Direttore Generale o Commissario Straordinario, la cui copia autentica, conservata presso l'U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali", deve contenere l'elencazione degli specifici compiti e istruzioni operative allo stesso impartite.

L'Amministratore di Sistema ha il compito di:

- Assicurare l'adozione di idonee misure di sicurezza dei sistemi informativi dell'ASP - PA adeguate al tipo di trattamento posto in essere;
- Rilasciare le credenziali iniziali agli Autorizzati del trattamento per l'accesso alle banche dati;
- Organizzare il database e gestire i flussi di dati e di rete;
- Vigilare affinché l'accesso alle banche dati dell'ASP - PA sia consentito solo al personale autorizzato e limitatamente alle proprie mansioni;
- Fornire supporto al Titolare e ai Responsabili del trattamento per l'individuazione, applicazione ed aggiornamento delle necessarie misure di sicurezza;
- Gestire eventuali incidenti e violazioni dei dati personali (**Data Breach**) in ambito informatico;
- Svolgere ogni altro compito previsto dalla legge o dai regolamenti.

L'operato dell'Amministratore di Sistema è soggetto, con cadenza almeno annuale, ad attività di **audit** da parte del Titolare in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

ART. 33 – GESTIONE INFORMATICA AZIENDALE

Viene nominato "Delegato/Designato" ai sensi dell'articolo 29 GDPR e dell'articolo 2-quaterdecies Codice Privacy, il Responsabile dell'U.O.C. "Gestione Informatica Aziendale", anche Responsabile della Sicurezza Informatica e Responsabile della Transizione Digitale che, secondo quanto prescritto dal Garante della Protezione dei Dati Personali nel provvedimento del 27 novembre 2008, pubblicato nella Gazzetta Ufficiale n. 300 del 24 dicembre 2008.

E' tenuto, oltre ai compiti previsti in qualità di Delegato/Designato di Struttura, a svolgere i seguenti ulteriori compiti:

- Nominare gli Amministratori di Sistema (ADS) interni, previa valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti che si intendono nominare, individuando per iscritto, per ciascuno di essi, le matrici dei sistemi di cui viene affidata l'amministrazione avendo cura di informare il R.P.D./D.P.O. e il Responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali";

- Tenere l'elenco aggiornato degli Amministratori di Sistema , ove devono essere riportate le funzioni a ciascuno di essi attribuite.
- Verificare, con cadenza almeno annuale, l'idoneità degli Amministratori di Sistema rispetto alle modifiche ai sistemi informativi ed ai ruoli assegnati, intercorse nel periodo, informando dell'esito di tali verifiche il R.P.D./ D.P.O.;
- Predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure tecnologiche relative alla sicurezza dei dati, rendicontando per iscritto in merito all'adeguatezza ed efficacia delle stesse al R.P.D./D.P.O.;
- Curare la tenuta e l'aggiornamento del registro degli asset informatici (licenze, applicativi e programmi in uso al personale), rendicontando per iscritto, con scadenza almeno semestrale, al R.P.D./D.P.O. e al Responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" , quest'ultimo al fine di curare l'aggiornamento del Registro dei Trattamenti;
- Curare la tenuta del registro degli incidenti di sicurezza, aggiornando per iscritto il R.P.D./ D.P.O.;
- Ove ritenuto necessario dal Responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" partecipare alla procedura valutativa, di cui alla "Procedura di applicazione del **Principio di Privacy by Design e Privacy by Default**", anche al fine della individuazione delle misure di mitigazione del rischio;
- Assistere il R.P.D./D.P.O. nelle interlocuzioni con il Garante della Protezione dei Dati Personali e nell'attuazione dei correttivi eventualmente indicati dallo stesso;
- Coordinare d'intesa con il Responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" ed il R-P.D./D.P.O. il processo di notifica e le successive interlocuzioni con le autorità competenti AGID e CSIRT nell'ambito del processo di gestione del Data Breach;
- Collaborare e supervisionare i Delegati/ Designati delle strutture aziendali , ognuno per la propria competenza, nella gestione dei profili di abilitazione all'utilizzo di applicativi e sistemi aziendali degli Autorizzati al Trattamento;
- Individuare i Responsabili del Trattamento ai sensi dell'art. 28 GDPR, con attribuzioni delle funzioni di Amministratore di Sistema, coordinandosi con i Delegati/Designati di Area Tecnico Amministrativa;
- Supervisionare l'effettiva realizzazione della verifica dell'operato degli Amministratori di Sistema, su base annuale, come previsto del citato Provvedimento e fino alla validità dello stesso e relazionare quindi il D.P.O. e il Responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" a riguardo;
- Ove risultasse necessario eseguire una Valutazione dell'Impatto del trattamento sulla protezione dei dati personali la "**DPIA"**, deve procedere se richiesto, in collaborazione con il Responsabile della U.O.S. "Data Protection Officer e Sistemi di Sicurezza nei Rapporti Istituzionali" e la partecipazione del Delegato/Designato della Struttura aziendale coinvolto nel flusso in esame e del D.P.O., alla redazione della stessa mediante l'utilizzo dell'applicativo indicato nelle "Linee guida DPIA".

I soggetti nominati Amministratori Di Sistema sono tenuti ad osservare le istruzioni indicate nel documento di "Nomina Autorizzati del Trattamento" e in aggiunta a quelle indicate nel documento di "Nomina Amministratore di Sistema" .

ART. 34 - SICUREZZA DEL TRATTAMENTO

Le misure di sicurezza devono "**garantire un livello di sicurezza adeguato al rischio**" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva.
Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al Responsabile in rapporto ai rischi specificamente individuati come da art. 32 del Regolamento.
Il Titolare e i Responsabili del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura di sicurezza necessaria per assicurare un livello sufficiente di sicurezza dei dati personali trattati.
Questi, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

Tali misure comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente disponibilità e accesso dei dati personali in caso di incidente;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'accesso a ogni procedura informatica è consentito solo se congruente con il trattamento dei dati per il quale si è stati formalmente autorizzati ed è consentito soltanto utilizzando apposite credenziali di autorizzazione fornite dall'Azienda strettamente personali e della cui riservatezza risponde personalmente il singolo soggetto autorizzato al trattamento dei dati personali.

In caso di trattamenti affidati a soggetti esterni all'Azienda, i responsabili del trattamento sono tenuti ad assicurare al titolare del trattamento di aver adottato, prima di effettuare ogni attività, ogni misura minima di sicurezza prevista dalla normativa vigente in materia di protezione dei dati e amministrazione digitale.
Il Data Protection Officer verifica, periodicamente in sede di audit, la congruenza della nomina ad Autorizzato con la richiesta di rilascio delle credenziali.

La password è strettamente personale e a nessun titolo può essere comunicata a terzi. Della sua riservatezza risponde personalmente il singolo Autorizzato del trattamento dei dati personali.
Il Delegato/Designato è tenuto a comunicare agli Amministratori di Sistema e al Data Protection Officer la data di cessazione dell'incarico al trattamento dei dati da parte del suo collaboratore.
L'ASP – PA adotta ed aggiorna, ogniqualvolta intervengano modifiche sostanziali, un **Documento di Analisi e Valutazione Rischi** (di seguito DAVR), che:

- Individua le misure adeguate a elevare lo standard di sicurezza dei dati anche sulla base dell'analisi dei rischi;
- Rappresenta la distribuzione dei compiti e delle responsabilità del trattamento dei dati;

- Evidenzia le misure che I' ASP . PA ha adottato nel tempo per proteggere i dati personali a sua disposizione e il piano delle azioni di miglioramento che intende adottare per l'anno in corso.

Il DAVR è predisposto dall' Ufficio Informatico aziendale, di concerto con la U.O.S." Data Protection Officer e Sistema di Sicurezza nei Rapporti Istituzionale"

I nominativi e i dati di contatto del Titolare e del DPO sono pubblicati sul sito web istituzionale dell'Azienda Sanitaria Provinciale di Palermo: www.asppalermo.org .

ART.35 - PROTEZIONE DEI DATI PERSONALI FIN DALLA PROGETTAZIONE (PRIVACY BY DESIGN) E PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA (PRIVACY BY DEFAULT)

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese "**Data Protection By Design And By Default**", 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.
Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE 2016/679) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

L'ASP – PA mette in atto misure tecniche e organizzative adeguate (**Allegato n°2**), già in fase precontrattuale, per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, sia per quanto riguarda, in particolare:

- la quantità dei dati personali raccolti;
- la portata del trattamento;
- il periodo di conservazione;
- l'accessibilità.

Tali misure garantiscono inoltre che, per impostazione predefinita, i dati personali siano accessibili solo alle persone autorizzate e limitatamente a quanto necessario per il periodo di trattamento.

ART. 36 - VALUTAZIONE DI IMPATTO SULLA PROTEZIONE (VIP) DEI DATI E LA CONSULTAZIONE PREVENTIVA CON L'AUTORITA' GARANTE

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE 2016/679 rispetto alla gestione degli obblighi dei Titolari, ossia il **rischio inerente al trattamento**. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36) 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.

L'ASP – PA prima di attivare un trattamento dei dati personali si assicura che sia effettuata una apposita valutazione preliminare dell'impatto delle operazioni di trattamento, avvalendosi e consultandosi, qualora necessario, con il proprio Data Protection Officer.

La Valutazione di Impatto preliminare viene effettuata nei casi e nei modi previsti dalle disposizioni vigenti, e contiene:

- una descrizione sistematica dei trattamenti previsti e delle finalità, compreso, ove applicabile, l'interesse legittimo perseguito all'AP - PA;
- una valutazione della necessità e proporzionalità dei trattamenti in base alle finalità;

- una valutazione dei rischi per i diritti e le libertà degli interessati;
- 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 Regolamento UE, tenuto conto dei diritti e degli interessi legittimi delle persone in questione.

Se necessario l'ASP – PA procede a un riesame per valutare se il Trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato, l'ASP - PA, prima di procedere al trattamento, consulta l'Autorità Garante Privacy.

L'ASP - PA, inoltre, attiva tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche individuate dall'Autorità Garante Privacy per il corretto trattamento dei dati, in modo particolare per quanto riguarda i trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi sanitari integrati.

ART. 37 - FORMAZIONE DEI DELEGATI, AUTORIZZATI DEL TRATTAMENTO DEI DATI ED AMMINISTRATORI DI SISTEMA

L'ASP - PA, nel rispetto dell'art.32 del GDPR "Sicurezza del Trattamento" prevede che il Titolare e il Responsabile del trattamento fanno sì che chiunque agisca sotto la propria autorità e abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento.

Nel Piano Annuale di Formazione, sono previste iniziative atte ad assicurare la formazione e il continuo aggiornamento di tutti gli Autorizzati al trattamento sui temi della protezione dei dati personali e sui diritti, doveri e adempimenti previsti dalla normativa vigente.

Per il personale di nuova assunzione, l'obbligo formativo, almeno in fase iniziale, potrà eventualmente essere soddisfatto attraverso la messa a disposizione della specifica documentazione di nomina quale soggetto Autorizzato prodotta dall'ASP – PA.

I Responsabili e dei Sub-Responsabili esterni del trattamento sono tenuti ad assicurare all'ASP – PA che gli Autorizzati e gli Amministratori di Sistema che svolgono attività di trattamento di dati personali su loro mandato siano formati e continuamente aggiornati. Le attività di formazione possono anche prevedere anche dei focus mirati su argomenti specifici indirizzati anche a singole unità di personale.

ART. 38 - VIOLAZIONE DEI DATI PERSONALI "DATA BREACH" – NOTIFICA E COMUNICAZIONE

Una violazione dei dati personali è "ogni infrazione alla sicurezza degli stessi che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento." La violazione dei dati è un tipo particolare di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del Regolamento UE 679/2016.

Ogni soggetto Designato/Delegato o Autorizzato al trattamento dei dati personali è tenuto a informare senza ingiustificato ritardo il Titolare, del possibile caso di una violazione dei dati personali, contattando il Responsabile della U.O.S. "Data Protection e Sistemi di Sicurezza nei Rapporti Istituzionali" e il R.P.D./D.P.O. inviando una specificazione comunicazione all'indirizzo e-mail rpd@asppalermo.org.

Ogni Interessato, utilizzando l'apposito indirizzo mail (direzionegenerale@asppalermo.org) può segnalare al Titolare e/o al Data Protection Officer R.P.D./D.P.O. (rpd@asppalermo.org), un possibile caso di una violazione dei dati personali.
L'ASP – PA provvede a notificare la violazione all'Autorità Garante Privacy 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 degli interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente. La notifica della violazione dei dati personali deve almeno:

- 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;
- 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;
- Descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

Nel caso in cui non sia possibile fornire le informazioni contestualmente, le stesse potranno essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Il Titolare del trattamento documenta qualsiasi violazione dei dati personali in un apposito registro delle violazioni di dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
Tale documentazione consente all'autorità di controllo di verificare il rispetto delle indicazioni di legge.

DISPOSIZIONI FINALI

ART. 39 - RESPONSABILITA' IN CASO DI VIOLAZIONE

Il mancato rispetto delle disposizioni in materia di protezione dei dati personali è punito con le sanzioni di natura amministrativa e di natura penale previste dagli artt. 166-172 del D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018 nonché con sanzioni di natura disciplinare per violazione dei regolamenti aziendali.

Il Responsabile del Trattamento risponde per danno causato se non ha adempiuto agli obblighi previsti dal Regolamento a lui specificatamente attribuiti o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal titolare del trattamento.

Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo a loro imputabile.

ART. 40 - ENTRATA IN VIGORE E PUBBLICITA'

Il presente Regolamento entra in vigore dalla data di adozione con atto deliberativo del Direttore Generale, in sostituzione di ogni precedente Regolamentazione interna nella medesima materia.
Il Regolamento verrà pubblicato sul sito Web aziendale istituzionale www.asppalermo.org (nell'apposita sezione dedicata alla "Privacy").

La sostituzione dei nominativi individuati nelle deliberazioni di nomina di funzioni varie indicate nel presente Regolamento non comporta l'esigenza di apportare formali modifiche allo stesso Regolamento.

ART. 41 - RINVIO A DISPOSIZIONI DI LEGGE

Per tutto quanto non espressamente previsto dal presente Regolamento si rinvia alla normativa vigente in tema di protezione dei dati personali e amministrazione digitale: Regolamento EU 679/2016 del 27/04/2016 e al D. Lgs. 196/2003 modificato dal D. Lgs. 101/2018 e ai provvedimenti specifici del Garante.
L' ASP - PA si riserva, inoltre, di adeguare, modificare o integrare il testo del presente Regolamento qualora per motivi organizzativi e/o la normativa e le direttive sopra citate lo rendano opportuno.

ALLEGATI

Si riportano i modelli utilizzati per le nomine, approvati dal Titolare, che ne dispone l'utilizzo per le finalità di organizzazione interna volte alla protezione dei dati personali di cui l' ASP - PA è Titolare.
I sopra citati modelli standard sono allegati al presente Regolamento e ne formano parte integrante e sostanziale.Tuttavia, gli allegati ovvero la modulistica di seguito indicata è gestita separatamente dal presente documento. Ciò al fine di consentire l'aggiornamento dei modelli senza prevedere l'aggiornamento dell'intero documento.
L'ASP - PA pertanto, si riserva la possibilità di modificare od integrare detti modelli a seguito di eventuali successive variazioni sia della normativa sia della peculiare attività della Struttura organizzativainteressata, nonché dello specifico ruolo ricoperto e/o dell'incarico conferito alla persona

ALLEGATI

- Informativa Privacy ASP – Palermo (All. 1)
- Linee Guida di Privacy By Design e By Default (All. 2)
- Modello Atto di Nomina di Delegato/Designato (All.3)
- Modello Atto di Nomina di Autorizzato (All.4)
- Modello Atto di Nomina di Responsabile (All.5)

INFORMATIVA PRIVACY
(ai sensi dell'art. 13 del Regolamento UE 2016/679 - GDPR)

Titolare del trattamento dei dati personali
L'Azienda Sanitaria Provinciale di Palermo (di seguito "ASP-PA"), con sede in Palermo (PA), via Giacomo Cusmano n. 24, 90141 - direzionegenerale@asppalermo.org -, in qualità di Titolare del Trattamento, tratterà i Suoi dati personali in conformità a quanto stabilito dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "GDPR"), che abroga la Direttiva 95/46/CE, e secondo quanto previsto dal Codice in materia di protezione dei dati personali Decreto legislativo 30 giugno 2003, n. 196 così come novellato dal Decreto legislativo 10 agosto 2018, n. 101.
Suddetto quadro normativo, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza ed al diritto di protezione dei dati personali.
Tutto ciò considerato, l'Azienda Sanitaria Provinciale di Palermo ai sensi dell'art. 13 del GDPR, in qualità di "Titolare" del trattamento è tenuta a fornirLe, una precisa informativa in riferimento ai dati personali che La riguardano anche al fine di ottemperare al principio di trasparenza.

Responsabile della Protezione dei dati personali (RPD)
Il Titolare ha nominato, ai sensi dell'art. 37 del GDPR, il Responsabile della Protezione dei dati (RPD) raggiungibile all'indirizzo rpd@asppalermo.org

Tipologia di dati trattati
Oltre ai suoi dati personali[1], la ASP-PA potrà trattare, particolari categorie di dati personali ai sensi dell'art. 9 del GDPR EU 2016/679, in particolare, dati relativi allo stato di salute[2] che potranno essere forniti direttamente da Lei o acquisiti attraverso documentazione sanitaria nel corso di accertamenti o visite, nonché dati genetici[3] per finalità di prevenzione, diagnosi, terapia, ricerca o per consentirLe una decisione libera ed informata.
Potranno inoltre essere trattati dati sanitari riguardanti i familiari della persona assistita, solo se strettamente indispensabili a giudizio del professionista sanitario responsabile delle cure della persona.

Finalità' del trattamento
I dati oggetto del trattamento, sia personali che quelli relativi allo stato di salute, verranno utilizzati esclusivamente per le finalità istituzionali connesse o strumentali all'attività del Titolare nei limiti stabiliti dalla legge o da regolamenti, e precisamente per seguenti finalità:

a. finalità legate alla cura
   a) attività di prevenzione, diagnosi, cura e riabilitazione, ivi compresi servizi diagnostici, programmi terapeutici e qualsivoglia altro servizio erogato dall'ASP di Palermo, in caso di: 1) prestazioni specialistiche ambulatoriali; 2) ricoveri ospedalieri; 3) ricoveri residenziali, anche attraverso sistemi di teleassistenza e telemedicina;
   b) altre attività sanitarie e socio-sanitarie, diverse da quelle indicate al precedente punto e comunque connesse alla salute degli utenti;

[1] Per "dato personale" si intende qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
[2] Per "dati relativi alla salute" si intendono i dati personali attinenti la 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;
[3] I "dati genetici" sono 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.

e) attività amministrative e di gestione operativa legate ai servizi forniti;

d) attività correlate alla fornitura di altri beni o servizi all'utente per la salvaguardia della salute (es. fornitura di protesi e ausili e presidi).

b. finalità legate alia ricerca scientifica e alla didattica

a) indagini epidemiologiche e statistiche, per fini di ricerca scientifica e/o per valutazioni inerenti la qualità e appropriatezza delle prestazioni, utilizzando dati anonimizzati;

b) attività didattiche e di formazione professionale dei medici, degli altri professionisti, dei volontari e degli studenti frequentanti i corsi di studio, nel rispetto del diritto all'anonimato del paziente, ovvero prive di dati identificativi.

Base giuridica del trattamento

Per i trattamenti effettuati per finalità di diagnosi, assistenza o terapia sanitaria o sociale, ovvero gestione dei sistemi e servizi sanitari e sociali, (di seguito "finalità di cura"), così come chiarito dal Provvedimento dell'Autorità Garante per la Protezione dei dati personali "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario" – 7 marzo 2019, non è richiesto il consenso del paziente, in quanto, ai sensi dell'art. 9 paragrafo 2 lett. h) del GDPR e degli articoli 2-septies e 75 del D.Lgs. 196/2003 così come modificato e integrato dal D.Lgs. 101/2018DPR, il trattamento è necessario per il raggiungimento delle finalità di cura ed è effettuato nell'ambito di una struttura sanitaria da professionisti soggetti a segreto professionale o da altra persona soggetta anch'essa all'obbligo di segretezza.

Inoltre, non è richiesto il consenso del paziente 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 preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare).

L'obbligo di acquisire il consenso permane per le ulteriori fattispecie di trattamento: Studi Clinici, Consenso alla comunicazione di informazioni sullo stato di salute, app mediche, costituzione del Dossier Sanitario, referti on-line, etc.

Modalità' di trattamento e conservazione

I dati saranno trattati nel pieno rispetto della normativa sopra richiamata, del segreto professionale e degli obblighi di riservatezza ai quali è tenuto tutto il personale dell'ASP-PA.

Le finalità sopra indicate prevedono lo svolgimento delle operazioni di raccolta, registrazione, conservazione e modificazione dei dati personali, mediante strumenti manuali ed informatici, con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza, la riservatezza, l'integrità e la disponibilità dei dati.

I dati potranno essere trattati con la collaborazione di soggetti terzi espressamente nominati dal Titolare quali Responsabili del trattamento ai sensi dell'art. 28 del GDPR.

I dati verranno trattati con modalità informatizzate nonché in formato cartaceo.

Comunicazione e destinatari dei dati

I dati personali trattati per le sole finalità sopra esposte potranno essere trasmessi ai soggetti cui la comunicazione è prevista per legge o per regolamento, o sulla base di rapporti giuridici in essere con la ASP-PA. In particolare, potranno essere comunicati:

- ad altre Aziende Sanitarie ed Ospedaliere ed alla Regione di appartenenza dell'utente;

- alle compagnie assicurative dell'Ente ed agli ulteriori soggetti coinvolti nella definizione delle pratiche di risarcimento, ad es., loss adjuster (legali, periti, etc.), per la tutela dell'Ente stesso e dei suoi operatori nelle ipotesi di responsabilità;
- ad altri soggetti pubblici (ad es. Regione e Comune) o privati (a cui siano affidati contrattualmente servizi da parte dell'ASP-PA), per finalità istituzionali (ad es. igiene, sanità pubblica, controllo assistenza e spesa sanitaria);
- all'Autorità Giudiziaria e/o all'Autorità di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.

I dati personali trattati non sono in nessun caso oggetto di trasferimento al di fuori dell'Unione Europea.

Tempi di conservazione dei dati

La documentazione cartacea relativa a referti e cartelle cliniche è soggetta a obbligo di conservazione illimitata come disposto dalla circolare del 19 dicembre 1986 n.900 2/AG454/260 del Ministero della Sanità.

Diritti dell'interessato

Ai sensi degli artt. da 15 a 22 del GDPR, Lei ha il diritto in qualunque momento di esercitare i citati diritti inviando una istanza alla sede del Titolare, all'attenzione del Responsabile della Protezione dei Dati personali, o mediante l'invio alla casella di posta elettronica:

- rpd@asppalermo.org;
- direzionegenerale@asppalermo.org

In particolare potrà chiedere al Titolare del trattamento l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi laddove applicabile, la limitazione del trattamento dei dati che la riguardano o di opporsi al trattamento degli stessi qualora ricorrano i presupposti previsti dal GDPR e comunque esclusivamente nei limiti previsti dalla normativa vigente in tema di tutela del lavoro.
Inoltre, potrà proporre un reclamo al Garante per la protezione dei dati personali, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità: www.garanteprivacy.it.

LA DIREZIONE AZIENDALE

Identificativo: EJ4A56035T02 rev.0

Data: 30/09/2021

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

CIG 827283603D

Azienda Sanitaria Provinciale di Palermo

Linee Guida di Privacy by Design e By Default

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo Divisione Sistemi per la Sicurezza SpA

IBM SpA

	Nome e Ruolo	Firma
Autore		
	Leonardo S.p.A.	
Verifica		
Approvazione		
Autorizzazione		

Approvazioni Aggiuntive

Azienda	Nome e Ruolo	Firma

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda
0	30/09/2021	Dott. Giuseppe Buttafuoco	Azienda Sanitaria Provinciale di Palermo

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autori
0	30/09/2021	Prima emissione	Leonardo S.p.A.

SOMMARIO

INDICE DELLE TABELLE

INDICE DELLE FIGURE

1 INTRODUZIONE

Il Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR EU 2016/679) ha introdotto requisiti particolarmente stringenti con riferimento alle misure di protezione dei dati personali. Il Titolare del Trattamento e il Responsabile (Fornitore esterno) del Trattamento devono adottare ed attuare misure di sicurezza di tipo tecnico ed organizzativo commisurate ai rischi per l'interessato. Ciò deve essere realizzato attraverso l'implementazione di un sistema di controllo interno che garantisca il principio di "*Data Protection by Design*"[1], implementando la protezione dei dati personali sin dal momento della analisi, progettazione, rilascio, oltre che nell'esecuzione del trattamento durante la fase di gestione ordinaria.

L'introduzione di tale principio (in aggiunta a quello di "*Data Protection by Default*"[2]) comporta che un nuovo sistema o servizio venga progettato in modo da garantire che tutte le fasi del ciclo di vita siano condotte nel rispetto dei requisiti e vincoli di sicurezza e protezione dei dati e delle informazioni, consentendo inoltre di affrontare in maniera proattiva i rischi legati al trattamento dei dati personali.

La protezione dei dati diventa quindi un requisito predefinito a priori in fase progettuale e non integrabile a posteriori per approssimazione o modifica.

Per far fronte alle difficoltà di determinare a priori la natura e i contenuti degli eventi che possano richiedere l'utilizzo del processo di Privacy by Design/by Default, è stata predisposta la presente linea guida, volta alla definizione di un frame work di riferimento per la Privacy by Design/by Default durante l'intero ciclo di vita delle soluzioni (organizzative, di processo, di servizio, tecnologiche, ecc.)

Nella redazione di tali linee guida sono state prese a riferimento le seguenti documentazioni:

- European Data Protection Supervisor (EDPS) - Opinion 5/2018;
- Agenzia per l'Italia Digitale (AGID) - Linea guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design;
- Agenzia per l'Italia Digitale (AGID) - Linee guida AGID per lo sviluppo del software sicuro;
- Agenzia per l'Italia Digitale (AGID) - Misure minime di sicurezza ICT per le pubbliche amministrazioni;

[1] Art. 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita), c.1: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati."

[2] Art. 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita), c.2: "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica."

- Framework Nazionale per la Cyber Security e la Data Protection;
- European Union Agency for Network and Information Security (ENISA) - Privacy and data protection by design – from policy to engineering;
- Information Commissioner's Officer (ICO) - Guide to the General Data Protection Regulation – Data protection by design and default;
- PRIPARE - per gli aspetti metodologici di Privacy and Security by Design;
- LINDDUN - per la modellazione delle minacce Privacy (threat modeling);
- Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita - Versione 2.0.

1.1 Scopo

Scopo del presente documento è illustrare il Processo Privacy by Design/by Default nell' Azienda Sanitaria Provinciale di Palermo per garantire l'osservanza di quanto disposto dal Regolamento (UE) 2016/679 (di seguito GDPR) e dal D.Lgs. 30 giugno 2003, n. 196 così come integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n.101.

1.2 Ambito di Applicabilità

Il presente documento si applica all' Azienda Sanitaria Provinciale di Palermo, con la finalità di garantire il rispetto degli adempimenti privacy prescritti dalla normativa sia per i trattamenti di dati personali di cui la stessa è Titolare sia Responsabile del Trattamento, ove designata.

2 RIFERIMENTI

2.1 Documenti Applicabili

Rif.	Codice	Titolo
DA-1.	--	Capitolato Tecnico – Parte Generale "Procedura ristretta, suddivisa in 4 lotti, per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"
DA-2.	--	Capitolato Tecnico – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)"
DA-3.	--	Offerta Tecnica – Lotto 2 "Procedura ristretta per l'affidamento dei servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi online e di cooperazione applicativa per le Pubbliche Amministrazioni (ID SIGEF 1403)" del 22 Dicembre 2014
DA-4.	--	Piano dei Fabbisogni
DA-5.	LCam20190000054779 REV 1.02	Progetto dei Fabbisogni del 30/01/2020
DA-6.	CIG 827283603D	Contratto Esecutivo

Tabella 1 – Documenti applicabili

2.2 Documenti di Riferimento

Rif.	Codice	Titolo
DR-1.	--	ISO/IEC 29134:2017(E) - Information technology — Security techniques — Guidelines for privacy impact assessment.
DR-2.	--	Regolamento (UE) 2016/679 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 che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).
DR-3.	--	Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101.
DR-4.	--	Decreto Legislativo 10 agosto 2018, n. 101. "Disposizione per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati e che

Rif.	Codice	Titolo
		abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).
DR-5.	--	Provvedimento del Garante per la protezione dei dati personali del 11 ottobre 2018, n. 467.

Tabella 2 – Documenti di riferimento

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

Vocabolo	Titolo
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 (art. 4.1, GDPR);
Dato giudiziario	Dati personali relativi a condanne penali e reati (art. 10, GDPR), ed in particolare, per l'ordinamento giuridico italiano, ai dati idonei a rivelare i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale;
Dato particolare	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 (art. 9, GDPR);
Destinatari	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 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT 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 (art. 4.9, GDPR);
Consenso	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 (art. 4.11, GDPR);
Disponibilità	Proprietà per cui un dato personale è accessibile e utilizzabile da parte di un'entità autorizzata;
Impatto	Risultato o effetto sui trattamenti di dati personali determinato dall'accadimento di un evento di minaccia;
Integrità	Proprietà di un dato personale di essere accurato e completo;
Misure di sicurezza (o contromisure)	Contromisura implementata con lo scopo di mitigare la probabilità di accadimento e/o l'impatto dell'evento rischioso;
Persona autorizzata al trattamento	La persona fisica che nell'espletamento delle attività di competenza del Responsabile del trattamento, gestisce dati personali, sensibili o giudiziari (art. 4.10, GDPR);
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

Vocabolo	Titolo
	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 (art. 4.4, GDPR);
Registro dei Trattamenti	il Registro ove sono riportati per ciascun Responsabile del Trattamento i dati personali trattati nella sua Direzione/Struttura;
Responsabile della protezione dei dati (RPD/DPO)	Il Responsabile della protezione dei dati nominato secondo le specifiche modalità di designazione previste dall'art. 37 del GDPR) a cui vengono affidati i compiti elencati negli art. 38 e 39 GDPR;
Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del Titolare del Trattamento (art. 4.8, GDPR) specificamente individuata da quest'ultimo
Rischio Attuale	Livello di rischio che residua, rispetto al Rischio Potenziale, in virtù delle azioni di mitigazione già in essere;
Rischio Potenziale (o Intrinseco)	Livello di rischio cui è esposto un trattamento di dati personali indipendentemente dalle misure di sicurezza poste in essere;
Riservatezza	Proprietà per cui un dato personale non è reso disponibile o rivelato a individui, entità o processi non autorizzati;
Soggetto Delegato	Persone fisiche, espressamente designati dal Titolare del Trattamento, a cui quest'ultimo ha attribuito specifici compiti e funzioni connessi al trattamento di dati personali e che operano sotto l'autorità e nell'ambito dell'assetto organizzativo del Titolare stesso (art. 2-quaterdecies, D.Lgs. 196/2003).
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 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 (art. 4.7, GDPR);
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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 (art. 4.2, GDPR).

Tabella 3 – Definizioni

3.2 Acronimi

Codice	Titolo
AgID	Agenzia per l'Italia Digitale
ASP-PA	Azienda Sanitaria Provinciale di Palermo
Amministrazione	Azienda Sanitaria Provinciale di Palermo

Codice	Titolo
CE	Contratto Esecutivo
CQ	Contratto Quadro
Fornitore	Vedi Raggruppamento
Raggruppamento	Raggruppamento Temporaneo di Impresa Leonardo Divisione Sistemi per la Sicurezza S.p.A. (nel seguito Leonardo), società mandataria, IBM S.p.A. (mandante), Sistemi Informativi S.p.A. (mandante) e Fastweb S.p.A. (mandante).
RTI	Raggruppamento Temporaneo di Impresa

Tabella 4 – Acronimi

4 PRIVACY BY DESIGN & BY DEFAULT

Il principio di **Privacy by Default** (protezione dei dati per "*impostazione predefinita*") è volto a garantire, attraverso il soddisfacimento dei requisiti di protezione dei dati espressi nel GDPR, che all'atto del trattamento siano attive tutte le misure tecniche e organizzative volte a soddisfare quanto disposto dal GDPR; la Privacy by Default garantisce che le logiche di minimo trattamento, pseudonimizzazione dei dati, trattamento sicuro dei dati siano applicate come impostazione predefinita (default) e che i diritti siano esercitabili dall'interessato senza restrizioni.

Il principio di Privacy by Default è alla base dello studio e la predisposizione delle misure di protezione dei dati e la verifica dell'efficacia delle stesse, garantendo che:

- il principio della priorità della privacy sia applicato di default a sistemi e applicazioni;
- l'interessato sia informato di quali dati vengono raccolti e del loro utilizzo, prima dell'inizio del trattamento;
- i dati non vengano resi disponibili, senza un'azione specifica, a un numero indeterminato di persone;
- il trattamento sia sempre limitato, senza che sia necessaria una successiva azione specifica di limitazione;
- non venga instillato un falso senso di sicurezza privacy al soggetto del trattamento;
- la comunicazione dei dati dell'interessato ad altri possa avvenire solo dopo il suo consenso;
- l'interessato abbia tutte le informazioni e gli strumenti necessari a esercitare i propri diritti.

La validazione dell'efficacia delle misure di protezione avviene attraverso l'esame dei risultati derivanti della raccolta e analisi di indicatori specifici e del loro andamento nel tempo.

Il processo di **Privacy by Design** (protezione dei dati "*fin dalla progettazione*") è volto a garantire che le misure tecniche, di processo e organizzative adottate nella protezione dei dati tengano presente, sin dalla fase di progettazione, il soddisfacimento dei principi e dei requisiti di protezione dei dati espressi nel GDPR, mediante:

- l'impiego di misure tecniche ed organizzative nell'implementazione dei principi di protezione dei dati;
- l'inserimento di controlli nelle attività di trattamento, in modo da garantire la tutela dei diritti e delle libertà delle persone fisiche.

La Privacy by Design richiede che:

- la protezione dei dati personali sia una componente essenziale dei sistemi, prodotti e servizi;
- i principi e i requisiti di protezione dei dati siano parte del disegno e implementazione di sistemi, servizi, prodotti e processi aziendali;
- vengano utilizzati solo fornitori che considerano la protezione dei dati parte integrante e non secondaria nella fornitura di sistemi, servizi, prodotti.

Il modello del **Processo di Privacy by Design / By Default** va applicato per riconsiderare le misure tecnico-organizzative adottate o che si è deciso di adottare ogni qual volta, ad esempio:

- vengano sviluppate strategie e/o politiche che abbiano implicazioni privacy;
- venga sviluppata, acquisita o modificata una tecnologia che comporti il trattamento di dati personali;
- venga sviluppato, acquisito o modificato un sistema IT, processo, servizio, prodotto che comporti il trattamento di dati personali;
- venga avviato o modificato un trattamento di dati personali.

Nel processo di Privacy by Design / By Default si possono individuare 4 fasi/livelli a copertura dell'intero ciclo di vita dei dati:

- **ANALISI**: In questa fase vengono analizzati gli obiettivi di sicurezza privacy del "Target" generico (es. software, applicazione, infrastruttura, servizio, processo, trattamento), con la finalità di analizzare le funzionalità del Target ed individuare i requisiti di sicurezza privacy di alto livello. Sulla base delle informazioni raccolte viene valutato se è necessario condurre o meno una valutazione del rischio PIA. In tal caso dovrà essere eseguita la PIA secondo il relativo Processo.
- **DISEGNO**: In questa fase vengono analizzati nel dettaglio i requisiti di alto livello individuati nella fase precedente e i rischi emersi dalle attività di analisi, con l'obiettivo di definire i requisiti tecnici e di sicurezza privacy necessari per garantire le funzionalità della soluzione analizzata e la sicurezza dei dati personali trattati.
- **IMPLEMENTAZIONE**: In questa fase viene implementata la soluzione richiesta seguendo i requisiti tecnici e di sicurezza precedentemente individuati e programmati, secondo linee guida formali e strutturate.
  La soluzione una volta implementata deve essere sottoposta, prima del suo rilascio in produzione, ad una attenta attività di revisione della sicurezza (valutazione della sicurezza sulla soluzione sviluppata) e test, al fine di verificare che le funzionalità ed il livello di sicurezza richiesti e progettati siano stati garantiti.
  Eventuali difformità andranno gestite in modo formale con valutazione del rischio residuo che comporta; se il rischio non è accettabile può essere reiterata la fase di DISEGNO.
- **ESERCIZIO E DISMISSIONE**: In questa fase, che comprende la erogazione del servizio in ambiente operativo e l'eventuale sua dismissione, vengono pianificate attività periodiche volte ad identificare e correggere eventuali vulnerabilità in modo preventivo e proattivo e in, caso di dismissione, la cancellazione sicura dei dati in accordo con quanto previsto dalla regolamentazione corrente, in termini di obblighi di conservazione.
  La soluzione è continuamente monitorata e migliorata, al fine di identificare prontamente i potenziali problemi o errori nonché individuare eventuali nuovi requisiti di sicurezza privacy emersi, legati anche a possibili esigenze evolutive, alla integrazione con nuove tecnologie, a nuovi aspetti obbligatori di sicurezza o normativi.
  Qualora, in questa fase, nascano delle nuove esigenze nel trattamento dei dati si torna nuovamente alla fase di analisi per individuare gli eventuali nuovi i requisiti privacy da implementare.

La figura sottostante illustra i 4 livelli del framework ora descritti e che caratterizzano il Processo di Privacy By Design /By Default.

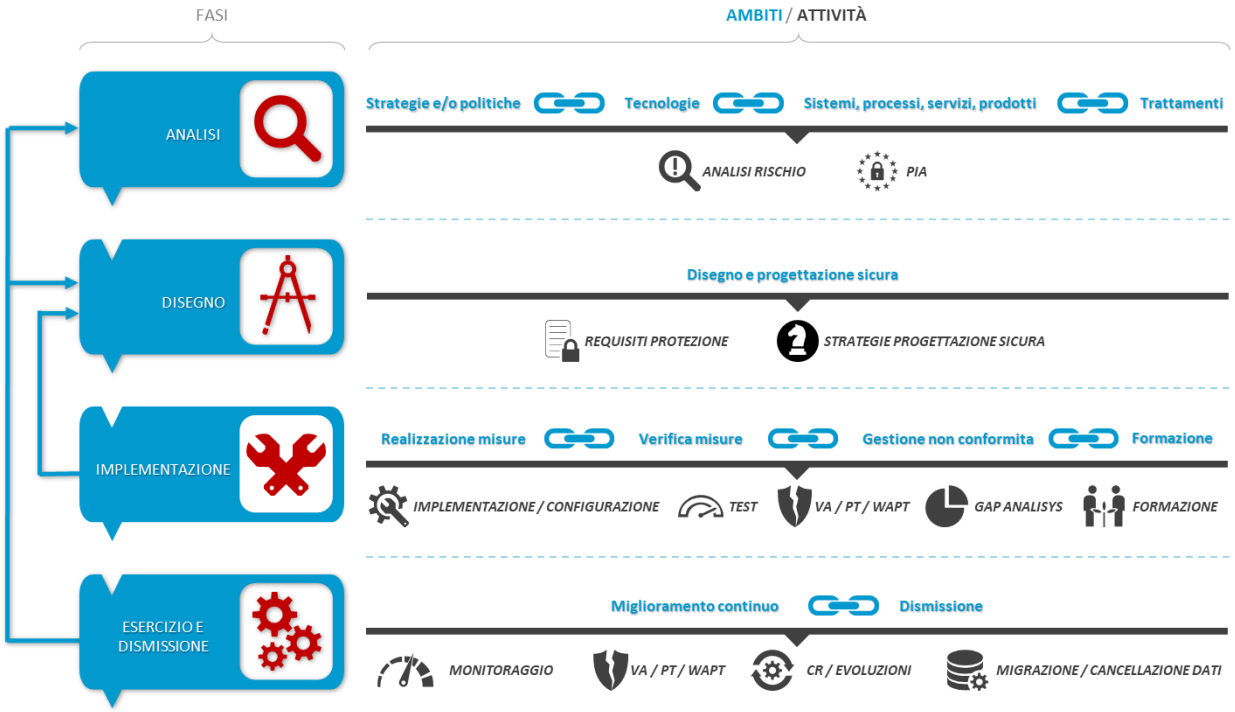

Figura 1 – Framework Privacy By Design / By Default

Di seguito e rappresentato il flusso di processo per la corretta implementazione della Privacy By Design /By Default.

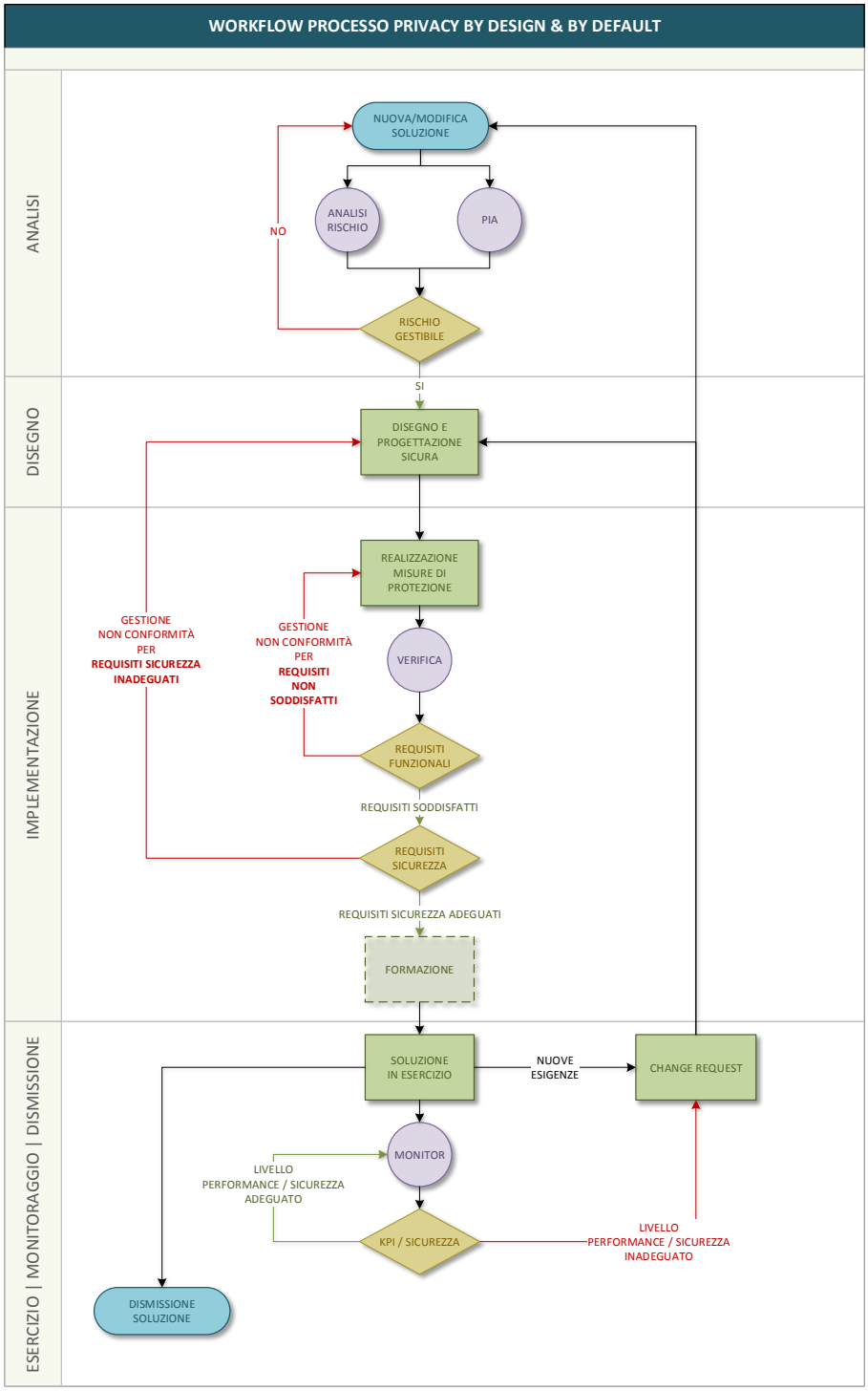

Figura 2 – Workflow Processo Privacy By Design / By Default

4.1 Attività e passi metodologici

4.1.1 Analisi

In funzione della tipologia di evento o dell'esigenza che ha causato l'attivazione del processo di Privacy by Design/Default viene eseguita l'attività specifica di valutazione dei rischi per la libertà e i diritti dei soggetti interessati. Sono di seguito riportati gli ambiti individuati per la fase:

- Strategie e/o politiche
- Tecnologie - ad esempio utilizzo di tecnologie cloud;
- Sistemi IT, processi, servizi, prodotti - ad esempio adozione di nuove piattaforme elaborative, nuovi servizi basati sulla esternalizzazione di attività istituzionali o di attività di supporto alle attività istituzionali;
- Trattamenti - ad esempio analisi massiva dei dati attraverso tecnologie di big data.

STRATEGIE E/O POLITICHE	
Obiettivo	Individuare i rischi che possono essere introdotti dall'adozione di nuove strategie/politiche o dalla modifica delle stesse.
Occorrenza	Ogni qual volta si verifichino dei cambiamenti normativi che abbiano effetti sulle strategie e/o politiche adottate dall'organizzazione con introduzione di nuovi rischi per la libertà e i diritti dei soggetti interessati.
Input *(elenco non esaustivo)*	• Regolamentazioni • Scenario/perimetro di utilizzo • Coinvolgimento di Terze parti • Flusso dei dati (DFD – Data Flow Diagram) • Minacce • Vulnerabilità • Scenari di rischio
Attività	• Analisi dei rischi • PIA
Guida all'attività	GDPR, Catalogo minacce, PRIPARE, LINDDUN, Opinion 5/2018 EDPS, ENISA Privacy and Privacy by Design, EDBP Opinion 12/2018
Owner (RACI)	**C** Responsabile per la Protezione dei Dati (RPD) **A/R** Soggetto Delegato al trattamento (es. UOC legale,...) **C** Servizio Informatico Aziendale **C** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

TECNOLOGIA	
Obiettivo	Individuare i rischi che possono essere introdotti dall'adozione di una nuova tecnologia o da modifiche nell'uso di una tecnologia già esistente.
Occorrenza	Ogni qual volta si vogliano adottare nuove tecnologie, o si utilizzano nuove funzionalità di tecnologie già in uso che possono introdurre nuovi rischi per la libertà e i diritti dei soggetti interessati.
Input ***(elenco non esaustivo)***	• Regolamentazione • Scenario/perimetro di utilizzo • Coinvolgimento di Terze parti • Tecnologie coinvolte • Flusso dei dati (DFD – Data Flow Diagram) • Minacce • Vulnerabilità • Scenari di rischio
Attività	• Analisi dei rischi • PIA
Guida all'attività	GDPR, Catalogo minacce, PRIPARE, LINDDUN, Opinion 5/2018 EDPS, ENISA Privacy and Privacy by Design, EDBP Opinion 12/2018
Owner (RACI)	**C** Responsabile per la Protezione dei Dati (RPD) **A/R** Servizio Informatico Aziendale **C** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

SISTEMI - PROCESSI - SERVIZI - PRODOTTI	
Obiettivo	Individuare i rischi che possono essere introdotti dall'adozione di nuovi sistemi (es. nuovi pacchetti applicativi), servizi (es. servizi di storage in cloud) o prodotti di trattamento dei dati (es. videosorveglianza) o modifiche degli stessi.
Occorrenza	Ogni qual volta si vogliano adottare nuove piattaforme tecnologiche o vengano aggiornate in modo significativo quelle esistenti, si vogliano acquisire nuovi sistemi di trattamento dati, si vogliano attivare nuovi servizi che interessano il trattamento dei dati, si voglia fare ricorso a servizi esterni per il trattamento dei dati dal punto di vista di processo e/o tecnologico. Esempi significativi possono essere: aggiornamento sistemi elaborativi, nuove piattaforme tecniche di gestione dati, nuovi sistemi di backup, servizi di condivisione dati, servizi esterni di sicurezza, esternalizzazione attività/processi/trattamenti.
Input ***(elenco non esaustivo)***	• Regolamentazione • Scenario/perimetro di utilizzo • Coinvolgimento di Terze parti • Sistemi, processi, servizi, prodotti coinvolti

SISTEMI - PROCESSI - SERVIZI - PRODOTTI	
	• Flusso dei dati (DFD) • Minacce • Vulnerabilità
Attività	• Analisi dei rischi • PIA
Guida all'attività	GDPR, Catalogo minacce, PRIPARE, LINDDUN, Opinion 5/2018 EDPS, ENISA Privacy and Privacy by Design, EDBP Opinion 12/2018
Owner (RACI)	**C** Responsabile per la Protezione dei Dati (RPD) **A/R** Servizio Informatico Aziendale **C** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

TRATTAMENTI	
Obiettivo	Individuare i rischi che possono essere introdotti dall'esecuzione di nuovi trattamenti o dalla necessità di utilizzare nuovi dati per l'esecuzione di uno o più trattamenti.
Occorrenza	Ogni qual volta si vogliano eseguire nuovi trattamenti sui dati personali o si voglia ampliare la quantità di dati da acquisire per adeguare alcuni trattamenti a nuove esigenze, anche in conseguenza di variazioni normative. Esempi significativi possono essere: nuovo trattamento (procedura), acquisizione di nuove informazioni per il rispetto di un obbligo di legge.
Input *(elenco non esaustivo)*	• Regolamentazione • Scenario/perimetro di utilizzo • Coinvolgimento di Terze parti • Informazioni sul trattamento e natura dei dati • Tecnologie coinvolte • Flusso dei dati (DFD) • Minacce • Vulnerabilità
Attività	• Analisi dei rischi • PIA
Guida all'attività	GDPR, Catalogo minacce, PRIPARE, LINDDUN, Opinion 5/2018 EDPS, ENISA Privacy and Privacy by Design, EDBP Opinion 12/2018
Owner (RACI)	**A/R** Responsabile per la Protezione dei Dati (RPD) **C** Soggetto Delegato al trattamento **C** Servizio Informatico Aziendale

TRATTAMENTI	
	C Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

4.1.2 Disegno

Dal profilo di rischio emerso in fase di analisi si derivano: le misure di protezione dei dati, le misure di protezione dei sistemi IT di supporto del trattamento, le misure a livello organizzativo e di processo.

Nel caso che la natura del trattamento comporti l'innalzamento del livello di rischio, o la presenza di nuove minacce da mitigare, occorrerà identificare le misure aggiuntive da adottare a protezione dei dati e degli interessati.

DISEGNO E PROGETTAZIONE SICURA	
Obiettivo	Adottare strategie e Best Practices per il disegno e la progettazione sicura delle soluzioni; selezionare le misure di protezione dei dati tra quelle disponibili o identificare le nuove misure necessarie per la protezione, atte a contrastare i rischi individuati nella fase precedente.
Occorrenza	A valle delle attività eseguite nella fase precedente
Input *(elenco non esaustivo)*	• Risultati Analisi dei rischi/PIA • Tecnologie coinvolte • Sistemi, processi, servizi, prodotti coinvolti • Informazioni sul trattamento e natura dei dati • Requisiti di protezione
Attività	• Definizione dei i requisiti di protezione dei dati • Definizione delle strategie e metodologie di progettazione sicura delle soluzioni
Guida all'attività	Classificazione delle informazioni, Misure minime di sicurezza AGID, Linee guida AGID per lo sviluppo del software sicuro, AGID Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del security/privacy by design, PRIPARE, LINDDUN, ENISA Privacy and Data protection by Design
Owner (RACI)	**C** Responsabile per la Protezione dei Dati (RPD) **C** Soggetto Delegato al trattamento **A/C** Servizio Informatico Aziendale **R** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività.

DISEGNO E PROGETTAZIONE SICURA	
	Informed (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

4.1.3 Implementazione

Implementazione delle misure di protezione dei dati individuate nella fase precedente e verifica e validazione, prima del rilascio della soluzione in produzione, della corretta progettazione e implementazione delle misure; eventuali difformità, emerse in fase di test, andranno gestite in modo formale con valutazione del rischio residuo e con l'eventuale reiterazione della fase di DISEGNO.

Nell'implementazione si fa ricadere anche la formazione del personale.

Sono di seguito riportati gli ambiti individuati per la fase:

- Realizzazione misure di protezione
- Verifica delle misure implementate
- Gestione delle non conformità
- Formazione

REALIZZAZIONE MISURE DI PROTEZIONE	
Obiettivo	Realizzazione delle nuove misure per adeguare il sistema di protezione e trattamento dei dati al nuovo profilo di rischio.
Occorrenza	Ogni qual volta debbano essere implementate le misure di sicurezza identificate nella fase precedente
Input ***(elenco non esaustivo)***	• Implementazione • Specifiche e requisiti di protezione • Fabbisogni tecnici • Piano di sviluppo-adeguamento-integrazione
Attività	• Implementazione e/o configurazione sistemi e/o servizi e/o applicazioni • Esecuzione del piano di sviluppo-adeguamento-integrazione nuove misure
Guida all'attività	Indicazioni tecnologiche-operative delle soluzioni adottate, Standard OSSTM e OWASP, CIS CONTROL (ex-SANS20), politiche, procedure, disposizioni normative.
Owner (RACI)	**I** Responsabile per la Protezione dei Dati (RPD) **I** Soggetto Delegato al trattamento **A/C** Servizio Informatico Aziendale **R** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

VERIFICA MISURE DI PROTEZIONE	
Obiettivo	Verifica che le misure logiche/fisiche implementate soddisfino i requisiti di protezione espressi nella fase DISEGNO.
Occorrenza	Al termine della fase di implementazione delle misure e prima dell'avvio in produzione
Input *(elenco non esaustivo)*	• Casi d'uso • Elenco nuove misure
Attività	• Test funzionalità logiche di protezione dei trattamenti e dei dati • Vulnerability Assessment & Penetration Test Infrastruttura (VA, PT) • Penetration Test Applicazione (WAPT)
Guida all'attività	Casi d'uso e criteri di accettazione
Owner (RACI)	**I** Responsabile per la Protezione dei Dati (RPD) **A/R** Servizio Informatico Aziendale **R** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

GESTIONE DELLE NON CONFORMITÀ RILEVATE DALLA VERIFICA	
Obiettivo	Gestione delle anomalie emerse dalle fasi di verifica logica e tecnica. La rilevazione di non conformità può comportare una revisione dell'implementazione o un ritorno alla fase di DISEGNO o alla Attività precedente di implementazione.
Occorrenza	Al termine delle fasi di verifica logica e tecnica.
Input *(elenco non esaustivo)*	• Elenco dei test falliti • Elenco delle vulnerabilità rilevate
Attività	• Valutazione della difformità e delle criticità rilevate in fase di test (GAP Analisys Funzionale/Sicurezza) • Quantificazione e valutazione del rischio residuo
Guida all'attività	Criteri di accettazione del rischio e Rischio atteso
Owner (RACI)	**I** Responsabile per la Protezione dei Dati (RPD) **A/R** Servizio Informatico Aziendale **R** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

FORMAZIONE	
Obiettivo	Adeguamento delle capacità operative del personale interno alle misure implementate.
Occorrenza	Qualora le misure impattino sulla operatività del personale
Input *(elenco non esaustivo)*	Fabbisogni formativi e organizzativi
Attività	Formazione personale interno
Guida all'attività	Politiche, Manuali metodologici e operativi, Piano di formazione
Owner (RACI)	**C** Responsabile per la Protezione dei Dati **I** Soggetto Delegato al trattamento **A/R** Servizio Informatico Aziendale **R** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

4.1.4 Esercizio e dismissione

L'approccio Privacy by Design/Default garantisce, durante la fase di esercizio, il corretto indirizzamento delle tematiche inerenti il Change Management, coerentemente con i requisiti Privacy.

Di seguito sono riportati gli ambiti individuati per la fase:

- Monitoraggio e miglioramento continuo
- Dismissione sicura delle soluzioni

MONITORAGGIO CONTINUO	
Obiettivo	Monitorare che la soluzione predisposta garantisca costantemente sia il soddisfacimento dei requisiti funzionali e di sicurezza, sia la rispondenza alle reali esigenze istituzionali e normative. Il mancato soddisfacimento di queste condizioni, può generare una Change Request (Richiesta di cambiamento) tale da reindirizzare il processo alle fasi di ANALISI e DISEGNO
Occorrenza	Attività continuativa ed iterativa per tutto il ciclo di vita della soluzione
Input *(elenco non esaustivo)*	• KPI in ambito privacy • Requisiti di sicurezza • Requisiti istituzionali e normativi
Attività	• Monitoraggio prestazioni e KPI in ambito privacy • Vulnerability Assessment & Penetration Test Infrastruttura (VA, PT) • Penetration Test Applicazione (WAPT) • Change Request / Evoluzione

MONITORAGGIO CONTINUO	
Guida all'attività	GDPR, Requisiti istituzionali e normativi
Owner (RACI)	**C** Responsabile per la Protezione dei Dati (RPD) **A/R** Servizio Informatico Aziendale **R** Fornitore esterno SEC/ IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

MIGLIORAMENTO CONTINUO	
Obiettivo	Monitorare che la soluzione predisposta garantisca costantemente sia il soddisfacimento dei requisiti funzionali e di sicurezza, sia la rispondenza alle reali esigenze istituzionali e normative. Il mancato soddisfacimento di queste condizioni, può generare una Change Request (Richiesta di cambiamento) tale da reindirizzare il processo alle fasi di ANALISI e DISEGNO
Occorrenza	Attività continuativa ed iterativa per tutto il ciclo di vita della soluzione
Input *(elenco non esaustivo)*	• KPI • Requisiti di sicurezza • Requisiti istituzionali e normativi
Attività	• Monitoraggio prestazioni e KPI • Vulnerability Assessment & Penetration Test Infrastruttura (VA, PT) • Penetration Test Applicazione (WAPT) • Change Request / Evoluzione
Guida all'attività	GDPR, Requisiti istituzionali e normativi
Owner (RACI)	**C** Responsabile per la Protezione dei Dati (RPD) **A/R** Servizio Informatico Aziendale **R** Fornitore esterno SEC/ IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

DISMISSIONE SICURA	
Obiettivo	Dismettere in modo sicuro soluzioni (tecnologie, sistemi, processi, servizi, prodotti, trattamenti) e garantire la cancellazione dei dati utilizzati non più necessari.

DISMISSIONE SICURA	
Occorrenza	Ogni qual volta si decide di abbandonare una specifica soluzione per il trattamento di dati o all'atto di un upgrade tecnologico; all'atto dell'eliminazione di trattamenti non più necessari o qualora famiglie di dati non siano più necessarie per i trattamenti, ad es. a seguito di variazioni normative; al termine della necessità di utilizzo dei dati.
Input ***(elenco non esaustivo)***	• Architettura tecnica • Architettura logica • Dati utilizzati sulla tecnologia in dismissione • Registro dei trattamenti
Attività	• Valutazione della necessità di conservazione dei dati utilizzati attraverso la tecnologia in dismissione o dal trattamento • Migrazione dei dati da conservare • Cancellazione sicura dei dati dai sistemi dismessi • Identificazione dei sistemi di memorizzazione coinvolti
Guida all'attività	Se disponibili, strumenti di data governance e data management.
Owner (RACI)	**I/C** Responsabile per la Protezione dei Dati (RPD) **I** Soggetto Delegato al trattamento **A/R** Servizio Informatico Aziendale **R** Fornitore esterno SEC/IT (Responsabile del Trattamento)
	Titolare del trattamento: ha la responsabilità di garantire in ciascuna fase del processo di privacy by design e by default il rispetto dei principi espressi nel GDPR. **Responsible** (R): è colui che esegue ed assegna l'attività **Accountable** (A): è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato. **Consulted** (C): è la persona che aiuta e collabora con il Responsabile per l'esecuzione dell'attività. **Informed** (I): è colui che deve essere informato al momento dell'esecuzione dell'attività.

REGIONE SICILIANA
AZIENDA SANITARIA PROVINCIALE DI PALERMO
DIREZIONE GENERALE

Prot. n._____ del _____

NOMINA DELEGATO/DESIGNATO AL TRATTAMENTO

Oggetto: ***Attribuzione di funzioni e compiti a soggetti designati al trattamento dei dati, in qualità di Delegati, ai sensi dell'art. 2 – quaterdecies del D.lgs. 196/2003 e ss.mm.ii., in conformità con il Regolamento (UE) 2016/679 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.***

Visto il Regolamento (UE) 2016/679 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 (di seguito indicato "**GDPR**"), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali.

Visto il D.Lgs. 30 Giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101, recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 (di seguito "**Codice Privacy e ss.mm.ii.**")

Considerato che lo svolgimento delle attività Istituzionali dall'Azienda Sanitaria Provinciale di Palermo comporta talora il trattamento di dati personali che sono tutelati dal GDPR, dal Codice Privacy e ss.mm.ii. nonché dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali (di seguito "**Normativa Privacy Applicabile")**

Considerato che, ai fini del GDPR per:

- *"Trattamento" si intende ai sensi dell'art. 4 del GDPR, "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"*

- *"Dato personale" si intende 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 (art. art. 4.1, GDPR);*

- *"Categorie particolari di dati personali" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché i dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, comma 1, GDPR);*

- *"Dati personali relativi a condanne penali e reati" si intendono i dati personali di cui all'art. 10 del GDPR.*

Preso atto che, ai sensi dell'art. 24 del GDPR, il Titolare del Trattamento è tenuto a mettere in atto le misure, tecniche ed organizzative, adeguare per garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente alla Normativa Privacy Applicabile;

Preso atto che l'art. 29 del GDPR stabilisce la regola generale per cui "*chiunque agisca sotto l'autorità del Responsabile del Trattamento o sotto quella del Titolare del Trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

Preso atto che l'art. 2-*quaterdecies* del Codice Privacy e ss.mm.ii. prevede esplicitamente che "*il Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*";

Preso atto che in tale contesto normativo, il Direttore Generale dell'Azienda Sanitaria Provinciale di Palermo, in qualità di Titolare del trattamento, ravvisa la necessità di nominare, all'interno della propria organizzazione, più Soggetti Delegati al Trattamento dei Dati Personali che lo affianchino al fine di garantire il pieno rispetto delle disposizioni dettate dalla Normativa Privacy Applicabile;

Preso atto che è stato designato il Responsabile della Protezione dei Dati Personali (RPD) dell'Azienda Sanitaria Provinciale di Palermo, in conformità a quanto prescritto dall'art. 37 del GDPR;

Consapevole che il Delegato effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e istruzioni;

Ritenuto che la S.V., per l'ambito di attribuzioni, funzioni e competenze conferite, abbia le garanzie sufficienti per mettere in atto tutte le misure tecniche ed organizzative adeguate a soddisfare i requisiti richiamati;

tutto ciò considerato, il Dott. _____. è designato/a:

SOGGETTO DELEGATO AI SENSI DELL'ART. 2 – *QUATERDECIES* DEL D.LGS. 196/2003 E ss.mm.ii. AL TRATTAMENTO DEI DATI PERSONALI

relativamente alle attività istituzionali svolte nell'Ufficio che Ella dirige *<inserire ufficio>* e che implicano un trattamento di dati personali.

Sarà cura della S.V. verificare la corretta adozione di tutti i principi e di tutte le misure di sicurezza previste dal GDPR, Cordice Privacy e ss.mm.ii., dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali (di seguito per brevità anche "Garante") e dalla circolare AGID del 17 marzo 2017, n. 1/2017 e vigilare affiché l'Ufficio di cui è responsabile effettui trattamenti di dati personali a norma di legge.

In particolare la S.V dovrà attenersi al rispetto delle seguenti **istruzioni**:

- presiedere ai trattamenti di dati personali di competenza dell'Ufficio, la cui elencazione e descrizione, ivi compresa la tipologia di dati, finalità e categoria di interessati, è riportata nel "Registro delle attività di Trattamento" di cui all'art. 30 del GDPR, disponibile presso la sede dell'Azienda Sanitaria Provinciale di Palermo;

- trattare i dati con la dovuta diligenza secondo le comuni regole della prudenza e con la massima riservatezza al fine di impedire, che estranei non autorizzati prendano conoscenza dei Dati che vengono Trattati;

- trattare i dati personali per il solo perseguimento delle finalità istituzionali dell' Azienda Sanitaria Provinciale di Palermo e, comunque, per scopi:
  - *Determinati*, vale a dire che non è consentita la raccolta come attività fine a sé stessa.
  - *Espliciti*, nel senso che il soggetto interessato va informato sulle finalità del trattamento.
  - *Legittimi*, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

- organizzare, nell'ambito dell'Ufficio di propria competenza, le operazioni di trattamento in conformità con la *Normativa Privacy Applicabile* ed in accordo con le eventuali indicazioni scritte impartite dal Titolare dell'Azienda Sanitaria Provinciale di Palermo, assicurando l'applicazione del principio della "*Protezione dei dati fin dalla progettazione e protezione predefinita*" di cui all'art. 25 del GDPR, determinando i mezzi del trattamento e mettendo in atto le misure tecniche e organizzative adeguate, di cui all'art. 32 del GDPR, prima dell'inizio delle attività in conformità alle prescrizioni ricevute dal Titolare del Trattamento (***privacy by design***). Inoltre, dovrà essere adottata ogni misura adeguata, fisica e logica, atta a garantire che i dati personali siano trattati in ossequio al principio di necessità e che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (***privacy by default***);

- garantire che i dati personali di pertinenza del proprio ufficio siano:
  - *Esatti*, cioè, precisi e rispondenti al vero e, se necessario, aggiornati.
  - *Pertinenti*, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta.
  - *Completi*: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato.
  - *Non eccedenti* in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso.
  - *Conservati per un periodo non superiore a quello stabilito dalla normativa applicabile* per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi;

- segnalare al Titolare, senza ritardo alcuno, ogni circostanza potenzialmente lesiva per i diritti e le libertà dell'interessato;

- collaborare con il Titolare del Trattamento affinché siano garantiti tutti i diritti dell'interessato di cui al Capo III del GDPR. In particolare, dovrà attenersi ad ogni istruzione scritta impartita al riguardo dal Titolare;

- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dalla *Normativa Privacy Applicabile* relative all'Ufficio che la S.V dirige, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso dal Responsabile della Protezione dei Dati o da un altro soggetto incaricato;

- informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati personali, qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti;

- provvedere, in caso di trattamento di dati effettuato in violazione dei principi summenzionati e di quanto disposto dalla *Normativa Privacy Applicabile* e previa comunicazione al Responsabile della Protezione dei Dati (RPD), al "**blocco**" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa);

- individuare e, se presenti, nominare, con il supporto del Responsabile della U.O.S. "Data Protection Officer" (R.P.D.), le Persone Autorizzate al trattamento, che prestano la propria attività all'interno dell'Ufficio che la S.V. dirige, ivi compresa, laddove presenti, la designazione delle figure di Amministratore di Sistema;

- controllare l'operato delle Persone Autorizzate al trattamento nonché sensibilizzare le stesse sugli aspetti normativi ed organizzativi in materia di tutela dei dati personali, ivi compreso il rispetto delle norme comportamentali dettate dal Titolare del trattamento*;*

- garantire che i profili di accesso ai sistemi informativi da parte delle Persone Autorizzate al trattamento siano configurati anteriormente all'inizio del trattamento e nel rispetto regole previste dall'Azienda in tema di credenziali di autenticazione, nonché verificare, almeno una volta l'anno, che tali profili siano conformi con le mansioni svolte garantendo la pertinenza e non eccedenza dei trattamenti effettuati;

- garantire la segretezza delle credenziali di accesso (**username e password**) nonché la relativa custodia. Qualora avesse il sospetto che terzi siano venuti a conoscenza delle stesse, si dovrà informare immediatamente il Servizio Informatico Aziendale ovvero provvedere con la modifica delle stesse;

- provvedere a modificare la parola chiave (**password**) al primo accesso, secondo la password policy aziendale, ovvero rispettando la composizione di almeno otto caratteri alfanumerici, modificandola almeno ogni sei mesi, nel caso in cui si trattino dati di natura comune, o almeno ogni tre mesi, nel caso si trattino anche dati particolari e dati relativi alla salute. A tal proposito, si ricorda che la password deve formare un codice non banale e non aver alcun riferimento con i propri dati personali (nomi, indirizzi, date di nascita…) Suoi, di suoi parenti, amici, colleghi o comunque conoscenti;

- vigilare circa la corretta adozione di specifiche misure di sicurezza a protezione dei dati personali scambiati con soggetti fornitori di servizi nell'ambito di contratti sottoscritti dall' Azienda Sanitaria Provinciale di Palermo o nell'ambito di Protocolli di Intesa e Convenzioni con soggetti terzi;

- collaborare con l'Autorità Garante in caso di ispezioni al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati inerenti all'Ufficio di competenza;

- **comunicare tempestivamente e senza ingiustificato ritardo al Titolare e al RPD le eventuali violazioni dei dati o gli incidenti informatici** (***data breach***) che possono avere un impatto significativo sui dati personali, al fine di consentire all'Azienda Sanitaria Provinciale di Palermo di comunicare al Garante Privacy, **entro settantadue (72) ore dalla conoscenza del fatto**, tali eventi secondo quanto previsto nel GDPR e comunque in rispetto delle policy dell'Azienda Sanitaria Provinciale di Palermo sugli incidenti relativi alla sicurezza delle informazioni e alla violazione dei dati personali;

- nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, supportare il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in possesso del Soggetto Designato;

- mantenere aggiornato, per l'Ufficio di propria competenza, il "**Registro delle Attività di Trattamento**" di cui all'art. 30 del GDPR, cooperando con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4 del GDPR;

- su eventuale espressa richiesta del Titolare, collaborare per i trattamenti dell'Ufficio di propria competenza ed unitamente al Responsabile della Protezione dei Dati, allo svolgimento della valutazione d'impatto sulla protezione dei dati (PIA), conformemente a quanto prescritto dall'art. 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'art. 36 del GDPR;

- garantire che la protezione dei dati personali all'interno dell'Ufficio di propria competenza sia realizzata, in osservanza alle disposizioni impartite dal Titolare del trattamento, in base alle misure di sicurezza previste dall'art. 32 del GDPR ed adeguate a ridurre al minimo i rischi di distruzione, perdita o modifica anche accidentale o illegale, dei dati, e divulgazione, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- collaborare - in caso di modifica della normativa in materia di protezione dei dati personali e nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse - con il Titolare e con il Responsabile della Protezione dei Dati personali, affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti introdotti;

- assicurare sistematicamente che, in caso di allontanamento dal posto di lavoro, i contenitori degli archivi siano conservati in luoghi chiusi a chiave (es: armadi/locali serrati). Per quanto concerne gli archivi cartacei, l'accesso è consentito solo se previamente autorizzato dal Titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati, avendo particolare riguardo a:
  - i documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
  - atti e documenti contenenti dati particolari o giudiziari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo tale che a tali atti e documenti non possano accedere persone prive di autorizzazione;
  - atti e documenti contenenti dati particolari o giudiziari devono essere restituiti al termine delle operazioni affidate;
  - eventuali fotocopie o copie di documenti devono essere autorizzate e custodite con le stesse modalità dei documenti originali;

- utilizzare gli strumenti informatici assegnategli secondo quanto previsto dalle “Norme comportamentali per il corretto utilizzo dei sistemi informatici e dei telefoni e fax aziendali” (Prot. 2207/URP – 18 nov. 2008);

- assicurare che siano state compiute le operazioni di formattazione dell’hard disk In caso di sostituzione di computer utilizzati nell’ambito della struttura da Lei diretta.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Palermo,

Titolare del Trattamento
Azienda Sanitaria Provinciale di Palermo
IL Legale Rappresentante
IL Commissario Straordinario
Dott.ssa Daniela Faraoni

Per Accettazione, il Delegato al Trattamento dei Dati
Responsabile della UOC Dott.

Firma _____

AZIENDA SANITARIA PROVINCIALE
di PALERMO

Prot. n._____ del_____

NOMINA A SOGGETTO AUTORIZZATO

Oggetto: ***Nomina "Persone autorizzate al trattamento" di dati personali ai sensi degli artt. 28 paragrafo 3, lett. b), 29 e 32 paragrafo 4 del Regolamento UE 2016/679 (GDPR) e dell'art. 2-quaterdecies del D.Lgs. 196/2003 così come integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101, recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.***

Visto il Regolamento (UE) 2016/679 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 (di seguito indicato "**GDPR**"), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali.

Visto il D.Lgs. 30 Giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101, recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 (di seguito "**Codice Privacy e ss.mm.ii.**")

Considerato che lo svolgimento delle attività Istituzionali dell'Azienda Sanitaria Provinciale di Palermo comporta il trattamento di dati personali e dati personali particolari che sono tutelati dal GDPR, dal Codice Privacy e ss.mm.ii. nonché dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali (di seguito "**Normativa Privacy Applicabile")**

Considerato che, ai fini del GDPR per:

- *"trattamento"* si intende ai sensi dell'art. 4 del GDPR, *"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"*
- *"Dato personale"* si intende 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 (art. art. 4.1, GDPR);
- "*categorie particolari di dati personali*" si intendono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale nonché i dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, comma 1, GDPR);
- "*dati personali relativi a condanne penali e reati*" si intendono i dati personali di cui all'art. 10 del GDPR.

Preso atto che l'art. 29 del GDPR stabilisce la regola generale per cui "*chiunque agisca sotto l'autorità del Responsabile del Trattamento o sotto quella del Titolare del Trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

Preso atto che l'art. 2-*quaterdecies* del Codice Privacy e ss.mm.ii. prevede esplicitamente che "*il Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.*";

Preso atto che, alla luce dell'art. 30 del GDPR, l'Azienda Sanitaria Provinciale di Palermo ha proceduto alla predisposizione del "Registro delle attività di trattamento", riportante per ciascuna Unità Operativa le informazioni in ordine ai trattamenti effettuati dall'Azienda Sanitaria Provinciale di Palermo;

Preso atto che è stato designato il Responsabile della Protezione dei Dati Personali (RPD) del l'Azienda Sanitaria Provinciale di Palermo - in conformità a quanto prescritto dall'art. 37 del GDPR;

Ciò premesso,

il sottoscritto Dott. _____ RESPONSABILE DELL'UNITA' OPERATIVA _____, nominato dal Direttore Generale dell'Azienda Sanitaria Provinciale di Palermo, in qualità di Titolare del Trattamento, quale Delegato al trattamento, in conformità a quanto prescritto ai sensi dell'art. 2 – quaterdecies del D.lgs. 196/2003 e ss.mm.ii., nomina la S.V. _____ **,**

PERSONA AUTORIZZATA AL TRATTAMENTO

relativamente alle attività aziendali svolte nell'Unità Operativa, in conformità e nei limiti delle proprie competenze espresse in ordini di servizio e circolari dell'Azienda Sanitaria Provinciale di Palermo, in particolare:

- (indicare i trattamenti effettuati) _____
- (indicare i trattamenti effettuati) _____

I trattamenti effettuati dalla suddetta Unità Operativa sono quelli riportati nel "Registro delle attività di trattamento" predisposto dall'Azienda Sanitaria Provinciale di Palermo ai sensi dell'art. 30 del GDPR e disponibile per la consultazione presso la sede del Titolare.

In questo ambito l'autorizzato dovrà rispettare le seguenti disposizioni:

- nel trattare i dati personali deve operare garantendo la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati personali confidenziali e, di norma, soggetti ad un dovere di riservatezza. Pertanto, non si dovranno divulgare a terzi le informazioni di cui si è venuti a conoscenza;
- trattare i dati in modo lecito e secondo correttezza;
- adottare tutte le misure necessarie a verificare l'esattezza dei dati raccolti e registrati, e se necessario, correggerli ed aggiornarli di conseguenza;
- comunicare tempestivamente e senza ingiustificato ritardo al Delegato e/o in assenza direttamente al Titolare ed al RPD le eventuali violazioni dei dati o gli incidenti informatici (data breach) che possono avere un impatto significativo sui dati personali, al fine di consentire all'Azienda Sanitaria Provinciale di Palermo di comunicare al Garante Privacy, entro settantadue (72) ore dalla conoscenza del fatto, tali eventi secondo quanto previsto nel GDPR e comunque nel rispetto delle policy dell'Azienda Sanitaria Provinciale di Palermo sugli incidenti relativi alla sicurezza delle informazioni e alla violazione dei dati personali;
- mettere in atto tutti gli accorgimenti necessari per assicurare la riservatezza, l'integrità e la disponibilità dei dati trattati nel rispetto delle disposizioni impartite dall'Azienda Sanitaria Provinciale di Palermo;

- adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso della persona Autorizzata; in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'Autorizzato dovrà verificare che non vi sia possibilità, da parte di terzi, di accedere a dati personali per i quali sia in corso un qualunque tipo di trattamento, sia cartaceo che informatizzato.
  In particolare, per chiunque abbia accesso a sistemi/applicazioni dell'Azienda Sanitaria Provinciale di Palermo, dovranno essere osservate le seguenti disposizioni:
  - le viene fornito, dalla Direzione ICT, un codice di identificazione (username), che dovrà provvedere a mantenere segreto. Qualora avesse il sospetto che terzi siano venuti a conoscenza dello stesso, dovrà informare immediatamente il Delegato al trattamento di riferimento;
  - le viene fornita una parola chiave (password), composta da otto caratteri alfanumerici che dovrà provvedere a modificare in occasione del primo accesso, e successivamente almeno ogni sei mesi, nel caso in cui lei tratti solo dati di natura comune, o almeno ogni tre mesi, nel caso in cui Lei tratti anche dati particolari e dati relativi alla salute. Le raccomandiamo di fare uso di caratteri alfanumerici, che formano un codice non banale e che non abbia alcun riferimento con i propri dati personali (nomi, indirizzi, date di nascita…) Suoi, di suoi parenti, amici, colleghi o comunque conoscenti;
  - la parola chiave deve essere da Lei mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia;
- svolgere le sole operazioni di trattamento consentite e conformi ai fini istituzionali per i quali i dati sono stati raccolti e trattati;
- collaborare con il Delegato per l'aggiornamento del "Registro delle attività di trattamento", di cui all'art. 30 del GDPR, e afferenti l'unità Operativa di appartenenza, laddove richiesto dal medesimo;
- comunicare tempestivamente, qualora necessario, al Delegato o al RPD dell'Azienda Sanitaria Provinciale di Palermo, ogni circostanza idonea a determinare un pericolo di dispersione o utilizzazione non autorizzata dei dati stessi nonché ogni evento legato a operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle definite dall'Azienda Sanitaria Provinciale di Palermo;
- le raccomandiamo di non disattivare i software di protezione di cui dispone la nostra organizzazione, le cui specifiche tecniche Le verranno fornite, oltre che in questa sede, ogni volta che vi sono dei significativi aggiornamenti. Sottolineiamo, in particolare, l'importanza di non aprire file di provenienza non certa o sospetta e di adottare diligentemente le opportune cautele, al momento della trasmissione all'esterno di nostri files (es. file in formato .zip protetto da password);
- per lo svolgimento delle Sue mansioni lavorative, Le verrà attribuita, se necessario, una casella di posta elettronica aziendale. Le raccomandiamo di utilizzarla esclusivamente per finalità legate alla Sua attività lavorativa ovvero secondo quanto previsto dalle "Norme comportamentali per il corretto utilizzo dei sistemi informatici e dei telefoni e fax aziendali" (Prot. 2207/URP – 18 nov. 2008);
- le verrà attribuito, se necessario, l'accesso ad Internet, del quale La invitiamo ad usufruire solo nei limiti necessari per lo svolgimento dell'attività lavorativa ovvero secondo quanto previsto dalle "Norme comportamentali per il corretto utilizzo dei sistemi informatici e dei telefoni e fax aziendali" (Prot. 2207/URP – 18 nov. 2008);
- le ricordiamo che è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore;
- prima di procedere al download di software, anche a titolo gratuito, non espressamente autorizzato dall'Azienda, dovrà inoltre chiedere l'autorizzazione al proprio Delegato del trattamento e Servizio Informatico Aziendale;
- per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati personali, può rivolgersi al Delegato al trattamento di riferimento per ricevere le opportune istruzioni.

Per quanto concerne gli archivi cartacei, l'accesso è consentito solo se previamente autorizzato dal Delegato o dal Titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati, avendo particolare riguardo a:

- i documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
- atti e documenti contenenti dati particolari o giudiziari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo tale che a tali atti e documenti non possano accedere persone prive di autorizzazione;
- atti e documenti contenenti dati particolari o giudiziari devono essere restituiti al termine delle operazioni affidate;
- eventuali fotocopie o copie di documenti devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

Ulteriori istruzioni rispetto a quelle elencate Le potranno, di volta in volta, essere fornite dal Titolare e/o dal Delegato al Trattamento, in base alla normativa applicabile.

La presente Autorizzazione è determinata ai sensi della normativa applicabile in materia di protezione dei dati personali, in considerazione delle mansioni già attribuite nel contratto di lavoro in essere con il Titolare.
Pertanto, resta inteso che la presente nomina avrà la medesima durata del suo rapporto con l'Azienda Sanitaria Provinciale di Palermo e che, successivamente alla cessazione dello stesso, Lei non sarà più autorizzato/a ad effettuare alcun tipo di trattamento sui dati e sarà, comunque, tenuto/a ad osservare il massimo riserbo su qualsiasi informazione o circostanza di cui fosse venuto/a a conoscenza nel corso del suo percorso lavorativo presso l'Azienda Sanitaria Provinciale di Palermo
Nel firmare la presente nomina, Lei si impegna formalmente all'obbligo legale di riservatezza dei trattamenti effettuati così come richiesto dal GDPR. Inoltre, si rende consapevole che l'inadempimento dell'obbligo di diligente e corretta esecuzione delle istruzioni ricevute in ordine a quanto sopra, ed in particolare la violazione del divieto di comunicazione e diffusione dei dati trattati, come sopra specificato, potrà costituire elemento di valutazione dell'attività svolta per conto dell'Azienda Sanitaria Provinciale di Palermo, Titolare del Trattamento dei Dati.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Distinti saluti,

data _____

_____
Il Delegato al trattamento
Unità Operativa _____
(nome e cognome Delegato al trattamento):_____

Per presa visione dell'autorizzazione ricevuta e accertamento della consapevolezza delle informazioni ricevute.

_____ _____
(Nome e Cognome) (firma)

Oggetto "Nomina a Responsabile del trattamento dei dati personali ai sensi degli artt. 4.8 e 28 del GDPR – Regolamento (UE) 679/2016 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".

Prot. n. _____/ Palermo lì_____

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI
Allegato al CONTRATTO N°..... DEL ...../..... /....., relativo alla DELIBERA N° ..... DEL ..../..../.....

TRA

L'Azienda Sanitaria Provinciale di Palermo con sede legale in via Giacomo Cusmano n.24 90141 Palermo, C.F. e P.I.V.A. n. 05841760829, nella persona del legale rappresentante pro tempore Dott.ssa Daniela Faraoni nonché in qualità di Commissario Straordinario;

E

La **<*indicare ragione e denominazione sociale della Società*>** **(**di seguito, per brevità, anche Società) con sede in ……in persona del legale rappresentante pro tempore Dott. ……;

PREMESSO CHE

L'Azienda Sanitaria Provinciale di Palermo, in qualità di **TITOLARE DEL TRATTAMENTO DI DATI PERSONALI,** svolge attività che comportano il trattamento di dati personali nell'ambito dei servizi istituzionalmente affidati;

L'Azienda Sanitaria Provinciale di Palermo, in qualità di Titolare del trattamento è consapevole di essere tenuto a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e di essere tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

VISTO che il Regolamento (UE) 2016/679 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 (di seguito GDPR), garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali;

VISTO il D. Lgs. 30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 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"* come novellato dal D. Lgs. 10 agosto 2018, n. 101 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 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"*;

PRESO ATTO che l'art. 4.2 del GDPR definisce «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;

PRESO ATTO che l'art. 4.7 del GDPR definisce "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;

PRESO ATTO che l'art. 4.8 del GDPR definisce "Responsabile del Trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

VISTO che le attività, erogate in esecuzione del Contratto **n°..... del ...../...../..... relativo alla Delibera n° ..... del ...../...../.....** in essere tra l'Azienda Sanitaria Provinciale di Palermo e ***<indicare ragione e denominazione sociale della Società>,*** implicano da parte di quest'ultima, il trattamento dei dati personali di cui è Titolare il Azienda Sanitaria Provinciale di Palermo, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;

VISTO che in data 24/12/2008 è stato pubblicato sulla Gazzetta Ufficiale il Provvedimento del Garante per la Protezione dei Dati Personali "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema", emanato in data 27/11/2008 e successivamente modificato ed integrato;

VISTO che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali;

VISTO che le "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni",* emanate dall'AgiD in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 (di seguito per brevità "*Misure minime AgID*"), hanno dettato le regole da osservare per garantire un uso appropriato dei privilegi di Amministratore;

VISTO che, ai sensi del comma 1 dell'art. 28 del GDPR, la Società presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui l'Azienda Sanitaria Provinciale di Palermo è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal GDPR;

Quanto sopra premesso, le parti stipulano e convengono quanto segue.

L'Azienda Sanitaria Provinciale di Palermo **NOMINA** ***<indicare ragione e denominazione sociale della Società>***, quale **RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** in virtù del presente atto di designazione, ai sensi e per gli effetti delle vigenti disposizioni normative contenute negli artt. 4.8 e 28 del GDPR, con riguardo alle operazioni di trattamento connesse all'esecuzione del suddetto contratto dichiara di essere edotta di tutti gli obblighi che incombono sul Titolare del trattamento e si impegna a rispettarne e consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica, attenendosi alle disposizioni operative contenute nel presente atto e di seguito enunciate:

- I trattamenti dovranno essere svolti nel pieno rispetto delle previsioni legislative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali. In particolare:
  - i trattamenti sono svolti ***<indicare le finalità per cui il fornitore tratta i dati ovvero l'oggetto del contratto>***;
  - i dati personali trattati in ragione delle attività di cui ai suddetti contratti hanno ad oggetto:
    - dati di natura personale (art. 4.1 GDPR);
    - dati sensibili (art. 9 del GDPR "Categorie particolari di dati personali");

- dati giudiziari (art. 10 del GDPR); ***<eliminare le eventuali tipologie di dati non oggetto di trattamento>***

- le categorie di interessati sono ***<indicare le tipologie di interessato (dipendenti/collaboratori) cui i dati afferiscono>*.**

- La Società si dichiara già in possesso di garanzie sufficienti per la messa in atto in termini di conoscenza specialistica, affidabilità e risorse, di misure tecniche ed organizzative adeguate a garantire che il trattamento dei dati soddisfi i requisiti del Regolamento UE 2016/679 nonché si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione predefinita" di cui all'art. 25 del GDPR (*privacy by design/default)*, a determinare i mezzi del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, di cui all'art. 32 del GDPR, prima dell'inizio delle attività.

- La Società dovrà eseguire i trattamenti funzionali alle attività ad essa attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, la Società dovrà informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo.

- La Società dovrà garantire in ogni caso l'obbligo di riservatezza; inoltre, i dati potranno essere trattati anche al fine di assolvere ad obblighi di legge, nonché nell'ambito delle proprie procedure interne in tema di controllo di qualità e gestione del rischio, da ritenersi inscindibilmente connesse e funzionali all'erogazione della prestazione professionale. Dette procedure sono finalizzate a presidiare il rispetto degli standard di qualità e indipendenza posti del Responsabile nel primario interesse del Titolare.

- La Società dovrà attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarle nei loro compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo anche in modo che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. La Società dovrà garantire, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza nonché che ricevano la formazione necessaria in materia di protezione dei dati personali.

- In particolare, tenuto conto dello stato dell'arte e dei costi di attivazione delle misure di sicurezza adottate a protezione dei trattamenti dei dati per conto del Titolare come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:
  - la pseudonimizzazione e la cifratura dei dati personali;
  - misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
  - procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- la valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

In aggiunta la Società, ove applicabile, dovrà adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID n. 2/2017 del 18 aprile 2017, nonché le eventuali ulteriori misure specifiche stabilite dal Titolare, nel rispetto dei contratti vigenti.

- La Società dovrà predisporre e tenere a disposizione della documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al Titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal GDPR, consentendo di effettuare periodicamente attività di verifica/audit, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato. Dette verifiche dovranno essere eseguite senza pregiudizio delle normali attività, in orari da concordare e con modalità che consentano il rispetto degli obblighi di riservatezza e confidenzialità nei confronti di altri soggetti e che in ogni caso non ledano o mettano in alcun modo in pericolo i segreti aziendali del Responsabile e/o il suo know-how. In alternativa, per l'esecuzione delle predette verifiche, il Responsabile potrà avvalersi di soggetti esterni di comprovata esperienza e trasmettere la risultanza al Titolare.

- La Società inoltre riconosce all'Azienda Sanitaria Provinciale di Palermo il diritto di effettuare controlli (Audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali del Titolare. A tal fine l'Azienda Sanitaria Provinciale di Palermo potrà periodicamente sottoporre alla Società un questionario sul livello di sicurezza e conformità alla normativa in materia dei dati personali (che dovrà essere debitamente compilato e restituito) e ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di Audit o di rendicontazione in ambito di protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile .

- Anche per le finalità sopraesposte, la Società è obbligata a mettere a disposizione in qualunque momento e su richiesta del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina ed è altresì tenuto a contribuire alle attività di revisione realizzate dal Titolare del trattamento o da un altro soggetto da questo incaricato, comprese le ispezioni

- La Società, ai sensi dell'art. 30 del GDPR e nei limiti di quanto esso prescrive, è tenuta a tenere un Registro delle attività di Trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4 del GDPR. Inoltre, la Società si impegna a comunicare al Titolare del trattamento ogni elemento utile per la predisposizione delle informazioni di cui agli art. 13 e 14 del GDPR.

- La Società è tenuta ad informare di ogni violazione di dati personali *(cd. data breach*), tempestivamente, e in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, il Titolare ed il Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo. Tale notifica – da effettuarsi tramite PEC da inviare sia all'indirizzo PEC del Titolare ***<indicare indirizzo PEC>*** - deve essere accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del GDPR, per permettere al Titolare, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. La società, dovrà fornire tutti i dettagli completi della violazione subita; in particolare: una descrizione della natura della violazione dei dati personali, le circostanze in cui è avvenuta, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali

sull'Azienda Sanitaria Provinciale di Palermo e sugli interessati coinvolti ed i provvedimenti adottati (o che si intendono adottare) per porvi rimedio ed attenuare i possibili effetti negativi, indicando il Responsabile della Protezione dei Dati (Data Protection Officer), con i relativi dati di contatto. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, la Società supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in suo possesso e/o di suoi sub-Responsabili.

- La Società, su eventuale richiesta del Titolare, è tenuto inoltre ad assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'art. 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'art. 36 del GDPR.

- La Società, qualora riceva istanze degli interessati in esercizio dei loro diritti di cui dall'art. 15 all'art. 22 del GDPR, è tenuta a:
  - darne tempestiva comunicazione scritta al Titolare o al Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo, allegando copia della richiesta;
  - valutare con il Titolare e con il Responsabile della Protezione dei Dati (RPD) del Azienda Sanitaria Provinciale di Palermo la legittimità delle richieste;
  - coordinarsi con il Titolare e con il Responsabile della Protezione dei Dati (RPD) del Azienda Sanitaria Provinciale di Palermo al fine di soddisfare le richieste ritenute legittime.

- La Società è autorizzata a nominare altri responsabili (di seguito, "Sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, necessarie all'esecuzione del contratto, e in tale ipotesi si impegna a rispettare le condizioni dell'art 28 del Regolamento EU2016/679 e conseguentemente a informare, a mezzo pec, il Titolare del Trattamento di eventuali modifiche previste al processo di trattamento riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche. Nella comunicazione andranno specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile del trattamento e i dati del contratto di esternalizzazione.

- La Società, nel caso in cui, per le prestazioni del Contratto **n°..... del ...../...../..... relativo alla Delibera n° ..... del ...../...../.....** che comportano il trattamento di dati personali, ricorra a subappaltatori o subcontraenti, è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al Titolare. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportati in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate, di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti.

- La Società deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante nel caso in cui siano inerenti il trattamento dei dati effettuato per conto del Titolare. Inoltre nel garantire gli adempimenti e le incombenze anche formali verso l'Autorità Garante quando richiesto e nei limiti dovuti, collabora tempestivamente, per quanto di competenza, sia con il Titolare sia con l'Autorità Garante per la protezione dei dati personali. In particolare:
  - fornisce informazioni sulle operazioni di trattamento svolte;
  - consente l'accesso alle banche dati oggetto delle operazioni di trattamento;

- consente l'effettuazione di controlli;
- compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.

- La Società si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato di cui agli artt. 40 e 42 del GDPR quando verranno emanati. Il Titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.

- La Società non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare. La Società si impegna a limitare gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server o in cloud) 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 GDPR (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello e etc.). Inoltre, la Società dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione, consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata del presente Contratto.

- La Società è obbligata altresì, a comunicare immediatamente all'Azienda Sanitaria Provinciale di Palermo il verificarsi di una delle seguenti fattispecie:
  - mancato rispetto delle clausole contrattuali standard di cui sopra; oppure
  - qualsiasi modifica della metodologia e delle finalità di trasferimento dei dati personali dell'Azienda Sanitaria Provinciale di Palermo fuori dalla Comunità Europea.

- La Società è tenuta a comunicare al Titolare ed al Responsabile della Protezione dei Dati (RPD) dell'Azienda Sanitaria Provinciale di Palermo il nome ed i dati del proprio RPD, laddove la società stessa lo abbia designato conformemente a quanto prescritto dall'art. 37 del GDPR. Il RPD collaborerà e si terrà in costante contatto con il RPD dell'Azienda Sanitaria Provinciale di Palermo. A tal fine il Titolare comunica al Responsabile che il proprio "Responsabile della Protezione dei Dati" è il Dott. Giuseppe Buttafuoco designato conformemente all'art. 37 del Regolamento UE, reperibile all'indirizzo mail: rpd@asppalermo.org

- La Società, ove applicabile, è tenuta a mettere in atto tutte le misure necessarie per ottemperare al provvedimento del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema", emanato in data 27/11/2008 e successive modifiche ed integrazioni. Ovvero si impegna a:
  - designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;
  - predisporre e conservare l'elenco contenente gli estremi identificativi delle persone qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
  - comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema;
  - verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica.

- La Società, ove applicabile, è tenuta a mettere in atto tutte le "misure minime di sicurezza ICT per le PP.AA." (livello minimo) prescritte dall'Agenzia per l'Italia Digitale (AgID) con Circolare n. 2/2017 del 18 aprile 2017.

- La Società, nel caso in cui, agisca in modo difforme o contrario alle legittime istruzione del Titolare oppure adotti misure di sicurezza inadeguate rispetto al rischio del trattamento sarà chiamata a rispondere delle inadempienze contrattuali secondo quanto stabilito nel contratto in essere tra le parti al quale la presente è allegata e parte integrante.
- Il Titolare del trattamento dichiara che tutte le comunicazioni inerenti i compiti, le funzioni e gli obblighi derivanti dal presente atto di nomina, gli potranno essere trasmesse ai seguenti riferimenti. PEC: direzionegenerale@pec.asppalermo.org o rpd@pec.asppalermo.org ; ovvero all'indirizzo della propria sede: Via Giacomo Cusmano n 24 - 90141 Palermo (PA).

  Il Responsabile del trattamento dichiara che tutte le comunicazioni inerenti i compiti, le funzioni e gli obblighi derivanti dal presente atto di nomina, gli potranno essere trasmesse ai seguenti riferimenti. PEC: ***<indicare indirizzo PEC>***.ovvero all'indirizzo della propria sede: ***<indicare indirizzo sede.>.***

La presente nomina avrà efficacia fino al termine del suindicato contratto in essere tra l'Azienda Sanitaria Provinciale di Palermo e la Società ovvero sino alla rinuncia o revoca del contratto in essere tra le parti.
All'atto della cessazione dei contratti in essere con l'Azienda Sanitaria Provinciale di Palermo, la Società, sulla base di quanto stabilito dal contratto, restituirà i dati personali oggetto del trattamento oppure provvederà alla loro integrale distruzione, salvo che i diritti dell'Unione e degli Stati membri ne prevedano la conservazione.
Tuttavia, la Società avrà facoltà di mantenere i dati trattati al solo fine di assolvere ad obblighi legali di conservazione e rispettare le proprie procedure in tema di documentazione dell'attività professionale svolta (ad esempio per richiesta di un'Autorità o in caso di contenzioso di qualsivoglia natura) salvo la conservazione della documentazione in ottemperanza delle normative vigenti quali a titolo esemplificativo quelle contabili e fiscali.

La validità del presente atto si intende altresì estesa ad ulteriori, eventuali, proroghe contrattuali; ogni altra pattuizione resta pienamente confermata e impregiudicata.

Il Titolare del Trattamento dei Dati

Azienda Sanitaria Provinciale di Palermo

(firma digitale)

Il presente atto deve essere firmato digitalmente dal Legale Rappresentante di ***<indicare Ragione sociale e riferimenti della Società>*** e inviato a mezzo PEC all'indirizzo direzionegenerale@pec.asppalermo.org e rpd@pec.asppalermo.org
Sottoscrivendo il medesimo atto, ***<indicare Ragione sociale e riferimenti della Società>***

(a) conferma di conoscere gli obblighi assunti in relazione alle disposizioni del GDPR e di possedere i requisiti di esperienza, capacità ed affidabilità idonei a garantire il rispetto di quanto disposto dal predetto decreto e sue eventuali modifiche ed integrazioni;
(b) conferma di aver compreso integralmente le istruzioni qui impartite e si dichiara competente e disponibile alla piena esecuzione di quanto affidato;
(c) accetta la nomina di Responsabile del trattamento dei dati personali e si impegna ad attenersi rigorosamente a quanto ivi stabilito, nonché alle eventuali successive modifiche ed integrazioni decise dal Titolare, anche in ottemperanza alle evoluzioni legislative in materia.

Timbro e firma digitale del Responsabile del Trattamento
(Legale Rappresentante della Società)

_____