|  |  |  |
| --- | --- | --- |
| **www.ausl.pe.it** | **Regione Abruzzo**  **ASL 03 Pescara** | **Regolamento Aziendale Privacy** |
| **LETTERA DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI**  **Art. 28 Regolamento UE 679/2016** | **Rev. 02/2018** |

Sede Legale:

Via Renato Paolini, 45

65124 Pescara

P. IVA 01397530982

**Il SOGGETTO AUTORIZZATO AL TRATTAMENTO**

**DI DATI PERSONALI CON DELEGA (SATD)**

Prot. n. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Pescara, lì \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Spett.le |  |
| Indirizzo: |  |
| CF/P.IVA |  |

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Ditta \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *Accordo per la Protezione dei Dati* (APD) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e della vigente normativa di settore. In applicazione della Delibera ASL PE n. \_\_\_\_\_\_\_\_ del \_\_/\_\_/\_\_.**

Il sottoscritto Dr. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_in qualità di Soggetto Autorizzato al Trattamento con Delega (di seguito anche SATD) della ASL di Pescara – Titolare del trattamento dei dati personali - considerato che:

1. La ASL di Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;
2. La nomina a Responsabile del Trattamento ai sensi dell’art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;
3. Il presente accordo integra e specifica gli obblighi derivanti dal Contratto allegato alla Delibera ASL PE n. \_\_\_\_\_\_\_\_ del \_\_/\_\_/\_\_ (di seguito la “Delibera”) tra la ASL di Pescara (di seguito “ASL PE” o “Titolare”) e la società \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (di seguito il “Fornitore” o il “Responsabile”) con particolare riferimento agli obblighi di protezione dei dati;

con il presente accordo designa

ai sensi dell’art. 28 del Reg. UE 679/2016 e

la società \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

quale Responsabile del Trattamento

dei dati personali trattati per conto della ASL di Pescara nell’ambito del servizio

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (oggetto della Delibera)

Il presente Accordo sulla Protezione dei Dati (di seguito anche APD) si applica a tutte le attività svolte dal Responsabile nell’ambito del trattamento dei dati personali ai sensi del Regolamento UE 679/2016 (di seguito “Regolamento” o “GDPR”), del D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali – di seguito “Codice” – come modificato dal D. Lgs. 101/2018) e della vigente normativa di settore, nell’ambito della Delibera, ivi comprese le attività svolte dai propri soggetti autorizzati al trattamento o terze parti (es.: sub-responsabili), nominate dal Responsabile, che trattino dati per conto del Titolare (ASL PE).

Di seguito verranno intesi il Responsabile e la ASL di Pescara congiuntamente come le "**Parti**" e ciascuna singolarmente come la "**Parte**"; inoltre ogni riferimento al Titolare dovrà essere inteso come effettuato al SATD ed ogni comunicazione al Titolare dovrà essere trasmessa congiuntamente al Soggetto Autorizzato con Delega scrivente (email: [\_\_\_\_\_\_\_\_\_\_\_\_\_\_@ausl.pe.it](mailto:______________@ausl.pe.it)), all’Ufficio Privacy (email: [ufficioprivacy@ausl.pe.it](mailto:ufficioprivacy@ausl.pe.it) ) ed al Responsabile della Protezione dei Dati (RPD o DPO, email: [dpo@ausl.pe.it](mailto:dpo@ausl.pe.it) ).

# Articolo 1 – Oggetto, natura, finalità e durata del trattamento

1. II presente APD si applica al trattamento dei dati personali svolto dal Fornitore in qualità di Responsabile del Trattamento per conto della ASL di Pescara, quale Titolare del Trattamento, ai sensi della Delibera e definisce gli obblighi delle Parti in materia di tutela dei dati personali;
2. La Natura, la finalità e l’ambito del trattamento sono definiti da tutti i trattamenti di dati personali effettuati nell’esecuzione dei servizi previsti dalla Delibera e riportati nell’Allegato 1 al presente Accordo sulla Protezione dei Dati (APD);
3. Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali;
4. Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.
5. La durata del trattamento dei dati personali dei Terzi Interessati da parte del Fornitore corrisponde alla durata riportata nella Delibera sulla base di quanto indicato nel Contratto;
6. Nell’Ambito di Trattamento definito, sarà compito del Responsabile fare in modo che i dati personali, trattati per conto del Titolare, siano:
   1. trattati in modo lecito, corretto e trasparente nei confronti dell’interessato («liceità, correttezza e trasparenza»);
   2. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
   3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
   4. 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 («esattezza»);
   5. 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 («limitazione della conservazione»);
   6. 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 («integrità e riservatezza»).

Le evidenze relative al rispetto del punto 6) sono riportate nell’Allegato 2 al presente documento.

# Articolo 2 – Tipologie di dati personali e categorie di interessati

1. I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente APD possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL, terzi incaricati, a qualunque titolo, dalla ASL, pazienti, controparti contrattuali della ASL e, in generale, terze parti rispetto alle quali la ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"), del Codice e della vigente normativa di settore. I dati personali trattati possono consistere, a titolo esemplificativo e non esaustivo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

# Articolo 3 – Istruzioni

1. Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell’Allegato 1 al presente APD. Il presente APD e la Delibera con i suoi allegati costituiscono parte delle istruzioni fornite dal Titolare per il trattamento dei dati personali, per il tramite del Soggetto Autorizzato al Trattamento con Delega, al Fornitore 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.
2. Qualsiasi istruzione aggiuntiva o modificata rispetto a quanto previsto nella Delibera e nel presente APD dovrà essere trasmessa dalla ASL al Fornitore per iscritto e comunicata via PEC e/o raccomandata a/r. Tale ulteriore istruzione diverrà efficace entro 30 giorni dalla data di comunicazione (invio).
3. Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Materiale didattico per la formazione e inoltre tutto quanto attinente alla materia pubblicato sul sito aziendale nella sezione Privacy.
4. È fatto obbligo al Responsabile di:
   1. Impegnarsi alla riservatezza secondo quanto previsto dall’art. 4 del presente APD;
   2. adottare le misure di sicurezza richieste ai sensi dell’Art. 32, come previsto dall’art. 5 del presente APD;
   3. fornire assistenza al Titolare del Trattamento secondo quanto previsto dall’art. 6 del presente APD;
   4. rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall’Art. 7 del presente APD;
   5. impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall’art.8 del presente APD;
   6. impegnarsi a supportare il Titolare nell’esecuzione della Valutazione di Impatto secondo quanto previsto dall’art.9 del presente APD;
   7. nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell’art. 28.3.b) del Reg. UE 679/2016 e dell’art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione come previsto dall’art. 10 del presente APD;
   8. ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell’art. 28 del Reg. UE 679/2016, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall’art. 11 del presente APD;
   9. ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall’art. 12 del presente APD;
   10. coadiuvare il Titolare nei rapporti con le autorità come previsto dall’Art. 13 del presente APD;
   11. rispettare gli ulteriori obblighi e responsabilità e le disposizioni finali secondo quanto previsto rispettivamente dagli artt. 14 e 15 del presente APD;
   12. redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento e degli eventuali sub-Responsabili e verificare annualmente l’ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell’assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);
   13. controllare le operazioni di trattamento svolte dagli autorizzati ed eventualmente dai sub-Responsabili e la conformità all’ambito di trattamento consentito;
   14. attuare gli obblighi di informazione (Informativa ex Artt. 13-14 del Regolamento) ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
   15. comunicare immediatamente al titolare non oltre le 12 ore successive al loro ricevimento (da parte propria o dei propri sub-Responsabili), ogni richiesta, ordine o attività di controllo da parte del Garante o dell’Autorità Giudiziaria;
   16. organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;
   17. rispettare tutto quanto ulteriormente disciplinato dal presente APD.

# Articolo 4 – Riservatezza

1. Il Fornitore si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
2. Il Fornitore garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto (Soggetti Autorizzati e Sub-Responsabili) si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

# Articolo 5 – Sicurezza del trattamento

1. Il Fornitore si impegna ad adottare tutte le misure richieste dall'Art. 32 del GDPR e le procedure tecniche e organizzative in materia stabilite dal Titolare.
2. In particolare - in considerazione dello stato dell'arte, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Fornitore si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 2 al presente APD di cui si richiede la compilazione per la descrizione delle modalità di implementazione.
3. Come ulteriore garanzia per la sicurezza del trattamento, il Fornitore si impegna a comunicare le informazioni riguardanti i prodotti e servizi forniti secondo quanto previsto dall’Allegato 3.
4. Qualora il Fornitore intendesse apportare modifiche alle misure tecniche e organizzative da lui descritte nell'Allegato 2 e/o alle indicazioni fornite nell’Allegato 3, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva idonea comunicazione, via posta elettronica ordinaria, al Soggetto Autorizzato con Delega sottoscritto e all’Ufficio Privacy, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure adottate in precedenza.

# Articolo 6 – Assistenza

1. Tenendo conto della natura del trattamento dei dati personali svolto dal Fornitore, come descritto nel Contratto allegato alla Delibera, il Fornitore si impegna 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 GDPR.
2. Il Fornitore dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti o di uno dei sub-responsabili (ved. Art. 11 del presente APD) uno dei diritti di cui agli Artt. da 15 a 22 del GDPR.
3. Tenendo conto della natura del trattamento, come descritto nel Contratto allegato alla Delibera e nel presente APD, e delle informazioni di volta in volta messe a disposizione, il Fornitore si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR.

# Articolo 7 – Conservazione, Riconsegna e Cancellazione

1. I dati personali trattati dal Titolare, che siano oggetto di trattamento da parte del Responsabile nell’ambito dell’esecuzione delle attività previste dal Contratto allegato alla Delibera, in base ai termini di conservazione previsti nei registri di trattamento, devono essere periodicamente cancellati dal Responsabile ove ne ricorra il termine. Alla cessazione del Contratto allegato alla Delibera, i dati oggetto di Trattamento da parte del Responsabile, per i quali non sia maturato il termine di cancellazione, devono essere restituiti al Titolare entro un termine massimo di 30 giorni dalla cessazione dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.
2. In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

# Articolo 8 – Violazioni di Dati Personali (cd. “Data Breach”)

1. Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai Dati Personali trasmessi, conservati o comunque trattati.
2. Il Responsabile si impegna inoltre, ai sensi dell’art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, 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 GDPR o di comunicazione della stessa agli interessati ai sensi dell’art. 34 del GDPR.
3. La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi [dpo.aslpe@pec.it](mailto:dpo.aslpe@pec.it) e [dpo@ausl.pe.it](mailto:dpo@ausl.pe.it).

# Articolo 9 – Valutazione D’impatto (CD. “DATA PROTECTION IMPACT ASSESSMENT”)

1. Il Responsabile, ai sensi dell’art. 28.3, lett. f), s’impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile, a fornire al Titolare ogni elemento utile all’effettuazione, da parte di quest’ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell’art. 35 del Regolamento, nonché ogni collaborazione nell’effettuazione della eventuale consultazione preventiva al Garante da parte di quest’ultimo ai sensi dell’art. 36 del Regolamento stesso.

# Articolo 10 – Soggetti Autorizzati al Trattamento

1. Il Responsabile garantisce che l’accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto e formalmente autorizzati (ex art. *2-quaterdecies* del Codice) , il cui accesso ai Dati Personali sia necessario per l’esecuzione dei Servizi.
2. Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, 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, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l’elenco aggiornato degli stessi.

# Articolo 11 – Sub-responsabili del Trattamento

1. Per l'esecuzione di specifiche attività per conto della ASL nell’ambito del Contratto, il Responsabile potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. 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 saranno 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 nel presente APD tra il 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. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.
2. Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell’art. 8 del presente APD), laddove intenda designare o sostituire un Sub-responsabile del Trattamento. La comunicazione al Titolare dovrà contenere l’elencazione dettagliata delle attività, previste dal Contratto, affidate al sub-Responsabile e dovrà essere effettuata 30 giorni prima dell’operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 30 giorni dalla ricezione della comunicazione da parte del Responsabile.
3. Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati nelle premesse e nell’art. 8 del presente APD), laddove intenda cessare il rapporto esistente con un sub-Responsabile del Trattamento senza procedere ad una sua sostituzione. Questa operazione prevede che le attività affidate al sub-Responsabile vengano riprese in carico da parte del Responsabile o riassegnate ad uno degli altri sub-Responsabili già nominati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 30 giorni prima dell’operazione di cessazione.
4. Qualora il Titolare sollevi obiezioni su uno o più Sub-responsabili del Trattamento, darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, quest’ultimo potrà:
5. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; o
6. adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
7. L'elenco completo ed aggiornato dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile per l'esecuzione di attività di trattamento dei dati di cui al Contratto allegato alla Delibera dovrà essere periodicamente (ogni anno entro il 31 gennaio) fornito al Titolare.
8. Il Fornitore è responsabile nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi previsti dalla normativa vigente in materia di Protezione dei Dati Personali e dal presente APD.
9. Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), 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.

# Articolo 12 – Amministratori di Sistema

1. Ove applicabile in relazione ai prodotti e servizi forniti, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell’Autorità.
2. In riferimento ai sistemi informatici (interni o esterni alle strutture dell’Azienda Sanitaria) di trattamento dei dati del Titolare, per i quali il Responsabile (o un suo Sub-responsabile) nomini uno o più Amministratori di Sistema (di seguito anche “AdS”), il Responsabile si impegna a:
3. 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, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
4. effettuare un’elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
5. predisporre e conservare l’elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
6. comunicare periodicamente (almeno una volta l’anno, entro il 31/01) al Titolare l’elenco aggiornato degli Amministratori di Sistema, specificandone l’ambito di responsabilità (sistemi, database, reti, applicativi, etc.) ed i dati di contatto per l’attivazione di eventuali procedure di emergenza;
7. comunicare tempestivamente (entro 3 giorni dall’ingresso, sostituzione o cessazione degli AdS) al Titolare eventuali variazioni che saranno riportate nell’elenco, specificando eventuali ingressi, sostituzioni o cessazioni, l’ambito di responsabilità (sistemi, database, reti, applicativi, etc.) e le eventuali credenziali di autenticazione introdotte o dismesse e, solo per i nuovi AdS, i dati di contatto per l’attivazione di eventuali procedure di emergenza;
8. verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
9. conservare i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili) o renderli disponibili per la conservazione da parte del Titolare (qualora i sistemi siano installati presso le strutture del Titolare);
10. garantire una rigida separazione dei compiti tra chi autorizza e/o assegna i privilegi di accesso (credenziali di Amministratore) e chi effettua le attività tecnico-sistemistiche sui medesimi sistemi.

# Articolo 13 – Rapporti con le Autorità

1. Il Responsabile, su richiesta del Titolare, si impegna a 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.

# Articolo 14 – Ulteriori Obblighi e Responsabilità

1. Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l’esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l’adempimento degli obblighi e delle istruzioni di cui al presente APD.
2. Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell’Audit.
3. Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell’Audit.
4. Il Responsabile si impegna altresì a:
5. effettuare almeno annualmente un rendiconto in ordine all’esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
6. collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l’intero processo di trattamento dei Dati Personali;
7. realizzare quant’altro sia ragionevolmente utile e/o necessario al fine di garantire l’adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
8. 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.
9. Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità (art. 28.10 del Regolamento).

# Articolo 15 – Disposizioni Finali

1. La presente designazione non comporta alcun diritto per il Responsabile 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 allegato alla Delibera.
2. Gli allegati al presente APD fanno parte integrante dello stesso: essi costituiscono parte integrante del Registro dei Trattamenti del Responsabile e dovranno essere mantenuti aggiornati da parte del Responsabile.
3. Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nel Contratto allegato alla Delibera.
4. Le comunicazioni che si intendono fatte annualmente da parte del Responsabile, devono essere inviate entro e non oltre il 31/01 di ogni anno.
5. Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente APD, costituisce una violazione del Contratto, di cui il presente APD è parte integrante, del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018) oltre che di quanto disposto dal Codice Civile e dal Codice Penale.
6. Il presente Accordo sulla Protezione dei Dati Personali deve essere restituito, opportunamente sottoscritto digitalmente entro 7 giorni dal ricevimento a mezzo PEC. La restituzione dovrà anch’essa essere effettuata a mezzo PEC all’indirizzo [protocollo.aslpe@pec.it](mailto:protocollo.aslpe@pec.it)
7. Una volta che il Fornitore abbia restituito il presente accordo a mezzo PEC, avrà a disposizione 30 giorni per la restituzione degli allegati 2 e 3 al presente APD. Tale termine per la compilazione degli allegati consentirà al Responsabile di poter indicare in maniera puntuale quanto richiesto e di essere eventualmente supportato (se richiesto) dal SATD e/o dal DPO in caso di necessità.
8. Gli allegati 2 e 3 al presente APD, forniti in formato editabile, dovranno essere restituiti da parte del Fornitore, compilati e sottoscritti digitalmente, inviandoli a mezzo PEC all’indirizzo [protocollo.aslpe@pec.it](mailto:protocollo.aslpe@pec.it).
9. Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

|  |  |  |
| --- | --- | --- |
| Il Soggetto Autorizzato al Trattamento con Delega (SATD) |  | Per ricezione ed integrale accettazione del Responsabile |
| Dr./ssa |  |  |
|  |  |  |

# ALLEGATO 1 – Ambito di Trattamento, Categorie di attività e Impatto

Scheda n.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nella scheda seguente (una per ogni trattamento), nell’ambito dei servizi erogati per conto della ASL di Pescara, vengono definiti i seguenti punti: l’ambito di Trattamento, le categorie di attività svolte dal Responsabile, e l’impatto sulla protezione dei dati; le informazioni sotto riportate sono necessarie per la compilazione dei Registri di Trattamento da parte del Responsabile (art. 30.2 del Regolamento).

|  |  |  |
| --- | --- | --- |
| **Cod.** | **Voce** | **Descrizione** |
| 1 | **AMBITO DI TRATTAMENTO** | |
| 1.1 | **Trattamento** |  |
| 1.2 | Finalità del trattamento |  |
| 1.3 | Categorie di interessati |  |
| 1.4 | Categorie di Dati Personali oggetto di trattamento |  |
| 1.5 | Categorie di Destinatari |  |
| 1.6 | Durata del trattamento |  |
| 1.7 | Durata della Conservazione |  |
| 1.8 | Trasferimento di dati personali verso un paese terzo o un’organizzazione internazionale |  |
| **2** | **CATEGORIE DI ATTIVITÀ RELATIVE AL TRATTAMENTO (OPERAZIONI DI TRATTAMENTO)** | |
| 2.1 | Raccolta |  |
| 2.2 | Registrazione |  |
| 2.3 | Organizzazione |  |
| 2.4 | Strutturazione |  |
| 2.5 | Conservazione |  |
| 2.6 | Adattamento o Modifica |  |
| 2.7 | Estrazione |  |
| 2.8 | Consultazione |  |
| 2.9 | Uso |  |
| 2.10 | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione |  |
| 2.11 | Raffronto o Interconnessione |  |
| 2.12 | Limitazione |  |
| 2.13 | Cancellazione o Distruzione |  |
| 2.14 | Trasferimento verso un paese terzo o una organizzazione internazionale |  |
| **3** | **VALUTAZIONE DI IMPATTO** | |
| 3.1 | Livello di Impatto Potenziale del Trattamento (prima dell’adozione delle misure di sicurezza previste nell’All.2) |  |
| 3.2 | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure indicate nell’All.2) |  |

Il livello di impatto indicato nella precedente tabella (punto 3) è relativo al valore valutato sia prima dell’adozione delle misure di sicurezza (riga 3.1 *“Livello di Impatto Potenziale”*), che successivamente all’implementazione delle stesse (riga 3.2 *“Livello di Impatto residuo”*).

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

* **1- Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
* **2 - Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
* **3 - Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e non oltre le 24 ore);
* **4 - Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell’interessato – es.: diritto alla salute)

# ALLEGATO 2 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei principi di trattamento, dei diritti degli interessati e l’adozione delle misure di sicurezza, secondo le indicazioni del Regolamento UE 679/2016, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) e del CNIL – (Garante francese per la protezione dei dati personali, indicato dal Garante italiano come riferimento per le attività di Valutazione di Impatto), nell’ambito delle attività svolte per conto del Titolare.

La decisione in merito all’applicabilità delle misure è del Titolare del Trattamento; nella seguente tabella è necessario dare opportuna indicazione dell’adozione di adeguate misure per il rispetto dei principi di trattamento e dei diritti degli interessati:

* Nel caso in cui la misura sia stata adottata, selezionare nel campo “Stato” la voce “A” per “Adottato” fornendo dettagli riguardanti la misura nel campo “Descrizione”.
* Nel caso in cui per l’attuazione della misura siano state programmate azioni con relative scadenze si prega di indicare nel campo “Stato” la voce “P” per “Programmato” fornendo dettagli e scadenze riguardanti la misura nel campo “Descrizione”.
* Nel caso in cui una misura sia ritenuta non adottabile o non prevista è necessario darne opportuna indicazione (nel campo Stato selezionando la voce “NP”) e motivazione (da indicarsi nel campo “Descrizione”).

Le indicazioni fornite nel presente allegato relative alle misure di sicurezza dovranno essere riportate all’interno del Registro dei Trattamenti del Responsabile.

## Principi di Trattamento e Diritti degli Interessati

| **Req.** | **Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)** | **Appl.**  *(SI/NO)* | **Stato**  *(****A****dottata*  */****P****ianificata*  */****N****on* ***P****revista)* | **Descrizione** |
| --- | --- | --- | --- | --- |
| A.1 | Art. 5.1.a – liceità | * SI * NO | * A * P * NP |  |
| A.2 | Art. 5.1.b – limitazione della finalità | * SI * NO | * A * P * NP |  |
| A.3 | Art. 5.1.c – minimizzazione dei dati | * SI * NO | * A * P * NP |  |
| A.4 | Art. 5.1.d – esattezza/qualità dei dati | * SI * NO | * A * P * NP |  |
| A.5 | Art. 5.1.e Limitazione della conservazione | * SI * NO | * A * P * NP |  |
| A.6 | Artt. 12, 13 e 14 – Informazioni per gli interessati | * SI * NO | * A * P * NP |  |
| A.6 | Art. 7 – Gestione del Consenso al Trattamento | * SI * NO | * A * P * NP |  |
| A.7 | Art. 15 Diritto di Accesso dell’interessato | * SI * NO | * A * P * NP |  |
| A.8 | Art. 16 – Diritto di Rettifica | * SI * NO | * A * P * NP | *Indicazione sia delle modalità operative per l’esercizio del diritto in questione* |
| A.9 | Art. 17 – Diritto alla Cancellazione (“Oblio”) | * SI * NO | * A * P * NP | *Indicazione sia delle modalità operative per l’esercizio del diritto in questione* |
| A.10 | Art. 18 – Diritto alla Limitazione del Trattamento | * SI * NO | * A * P * NP | *Indicazione sia delle modalità operative per l’esercizio del diritto in questione* |
| A.11 | Art. 19 – Obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento | * SI * NO | * A * P * NP | *Indicazione delle modalità operative per tenere traccia dei destinatari e garanzia dei diritti* |
| A.12 | Art. 20 – Diritto alla portabilità dei dati | * SI * NO | * A * P * NP | *Indicazione sia delle modalità operative per l’esercizio del diritto in questione* |
| A.13 | Art. 21 – Diritto di Opposizione | * SI * NO | * A * P * NP | *Indicazione sia delle modalità operative per l’esercizio del diritto in questione* |
| A.14 | Art. 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la *profilazione* | * SI * NO | * A * P * NP | *Indicazione delle modalità di gestione del processo decisionale automatizzato e delle modalità per garantire l’esercizio del diritto in oggetto.* |

## Misure di Sicurezza

Ai sensi degli Artt. 5.1.f), 25, 32 del Regolamento, si chiede di descrivere, secondo i criteri precedentemente esposti, quali delle seguenti misure tecniche e organizzative siano state adottate nell’ambito dei prodotti e/o servizi forniti al Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non adottabili e darne motivazione.

### Controlli Organizzativi

| **Req.** | **Misura** | **Dettaglio** | **Appl.** *(SI/NO)* | **Stato**  *(****A****dottata*  */****P****ianificata*  */****N****on* ***P****revista)* | **Descrizione**  *(Per alcune domande è possibile indicare più risposte)* |
| --- | --- | --- | --- | --- | --- |
| **CO.1** | **Politiche generali per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.2** | **Organizzazione per la protezione dei dati** | Articolazione dell’organizzazione per la Protezione dei Dati Personali (Soggetti Autorizzati, sub-Responsabili, ecc…) per il servizio fornito | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.3** | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell’organizzazione (RPD – DPO/Data Protection Officer) | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.4** | **Gestione della Sicurezza dei Dati trattati dalle risorse umane (dipendenti/collaboratori)** | Procedure di gestione dell’ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.  Piano di Formazione periodica sulla Protezione dei Dati Personali | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.5** | **Relazioni con i sub-fornitori** | Accordi, requisiti, procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.6** | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l’adeguamento del servizio alle nuove indicazioni  Procedure di Audit interne per assicurare la sicurezza dei trattamenti effettuati per conto dell’Azienda (test, verifica e valutazione dell’efficacia delle misure tecniche e organizzative) | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.7** | **Presenza di Polizza Cyber Risk** | Polizza cyber-risk ed eventuale dettaglio della stessa | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CO.8** | **Gestione del Cambiamento** | Procedura di gestione dei cambiamenti (Change Management) nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, di servizio o organizzativi, ecc…). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |

### Controlli per la Sicurezza dei Dati (CSD)

| **Req.** | **Misura** | **Dettaglio** | **Appl.** *(SI/NO)* | **Stato**  *(****A****dottata*  */****P****ianificata*  */****N****on* ***P****revista)* | **Descrizione**  *(Per alcune domande è possibile indicare più risposte)* |
| --- | --- | --- | --- | --- | --- |
| **CSD.1** | **Cifratura** | Procedure e Criteri di utilizzo della cifratura  *Misure per rendere i dati personali incomprensibili a chiunque non abbia un'autorizzazione di accesso (crittografia simmetrica o asimmetrica, uso di algoritmi pubblici noti per essere forti, certificato di autenticazione, ecc.).* | * SI * NO | * A * P * NP | Metodologia di Cifratura:   * nessuna * a livello Hardware (es.: Storage) * a livello Middleware (es.: DB) * a livello Software Applicativo * a livello protocollo di comunicazione * altra metodologia \_\_\_\_\_\_\_\_   Dettagli:   * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_): |
| **CSD.2** | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato (rif. art. 4.5 Reg. UE 679/2016) | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.3** | **Controllo degli accessi logici** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali  *Misure per limitare i rischi che persone non autorizzate accedano elettronicamente ai dati personali (gestione dei profili utente, meccanismi di autenticazione, politica delle password, ecc.).* | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.4** | **Controllo per il partizionamento - segregazione dei dati** | Procedure di gestione della segregazione dei dati | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.5** | **Tracciabilità (Logging)** | Procedure volte ad assicurare che la consultazione e l'azione svolta dagli utenti del trattamento siano registrate e attribuite, in modo tale che sia possibile fornire prove durante le indagini (sistema di registrazione, protezione, analisi, conservazione, ecc.). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.6** | **Monitoraggio dell'Integrità** | Procedure finalizzate ad essere avvisati in caso di modifica indesiderata o sparizione di dati personali (es.: funzioni di hash, codice di autenticazione dei messaggi, firma elettronica, prevenzione di SQL Injection, ecc.). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.7** | **Archiviazione** | Procedure per preservare e gestire gli archivi elettronici contenenti i dati personali destinati a garantire il loro valore (anche legale) | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.8** | **Sicurezza dei Documenti Cartacei** | Procedure per limitare i rischi di accesso di persone non autorizzate a documenti cartacei contenenti dati personali | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.9** | **Misure per il rispetto della Privacy by Design (Protezione dei dati fin dalla Progettazione)** | Ved. Reg. UE 679/2016 art. 25  *Indicare eventuali ulteriori misure adottate rispetto a quelle già indicate* | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSD.10** | **Misure per il rispetto della Privacy by Default (Protezione dei Dati per impostazione predefinita)** | Ved. Reg. UE 679/2016 art. 25  *Indicare eventuali ulteriori misure adottate rispetto a quelle già indicate* | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |

### Controlli per la Sicurezza Generale (CSG)

| **Req.** | **Misura** | **Dettaglio** | **Appl.** *(SI/NO)* | **Stato**  *(****A****dottata*  */****P****ianificata*  */****N****on* ***P****revista)* | **Descrizione**  *(Per alcune domande è possibile indicare più risposte)* |
| --- | --- | --- | --- | --- | --- |
| **CSG.1** | **Sicurezza Operativa** | Descrivere come vengano eseguiti gli aggiornamenti dei software (sistemi operativi, applicazioni, ecc.) e l'applicazione dei controlli correttivi di sicurezza (patches). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.2** | **Blocco dei Malware** | Indicare quale software antivirus/protezione sia installato e aggiornato a intervalli regolari sulle postazioni di lavoro e sui sistemi (anche server) forniti o sotto la propria responsabilità (anche per il supporto da remoto) nell’ambito del contratto. | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.3** | **Gestione delle postazioni di lavoro** | Descrivere le misure di sicurezza implementate sulle postazioni di lavoro utilizzate nell’ambito del servizio e sotto la propria responsabilità (blocco automatico con timer, firewall, ecc.). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.4** | **Sicurezza dei Siti Web** | Indicare se siano state implementate misure per la sicurezza dei siti Web facenti parte della fornitura | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.5** | **Backup** | Indicare le modalità di gestione dei backup (Piano di Backup) | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.6** | **Manutenzione** | Descrivere le modalità di gestione della manutenzione hardware ed indicare se questo sia tramite un contratto di subfornitura.  Indicare se siano possibili interventi di manutenzione da remoto e quali siano le misure di sicurezza adottate. | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.7** | **Sicurezza dei Canali Informatici (reti)** | Indicare il tipo di rete su cui sono eseguite le elaborazioni (isolata, privata o Internet).  Specificare quale sistema firewall, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi siano incaricati di garantire la sicurezza della retesotto la propria responsabilità | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.8** | **Monitoraggio (gestione incidenti)** | Indicare se sia implementato il monitoraggio del funzionamento/sicurezza dei sistemi forniti e con quali modalità. | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.9** | **Controllo degli accessi fisici** | Indicare quali siano le procedure di sicurezza per il controllo dell'accesso fisico alle strutture da cui viene erogato il servizio, che ospitano l'elaborazione o da cui venga effettuato supporto remoto (suddivisione in zone, scorta di visitatori, uso di pass, porte chiuse, videosorveglianza e così via). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.10** | **Sicurezza Hardware** | Indicare i controlli relativi alla sicurezza fisica dei server e delle workstation (archiviazione protetta, cavi di sicurezza, filtri di riservatezza, cancellazione sicura prima della rottamazione/ sostituzione, ecc.). | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.11** | **Continuità Operativa/**  **Disaster Recovery** | Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **CSG.12** | **Sicurezza dei sistemi applicativi/ ambienti operativi (anche di virtualizzazione o per la gestione del Cloud – acquisizione, manutenzione, sviluppo)** | Procedure/Misure di Sicurezza adottate per i sistemi applicativi o ambienti operativi forniti/utilizzati nella gestione dei sistemi/servizi oggetto del contratto con particolare riferimento a sviluppo, acquisizione, gestione operativa/protezione e manutenzione degli stessi | * SI * NO | * A * P * NP | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento tecnico allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |

# ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto

Fornire, ove indicate come applicabili rispetto al servizio fornito, le seguenti informazioni: si prega di indicare la risposta nell’apposito riquadro con eventuali documenti e/o schede tecniche da allegare.

| **Req.** | **Dettaglio** | **Appl.** *(SI/NO)* | **Descrizione**  *(Per alcune domande è possibile indicare più risposte)* |
| --- | --- | --- | --- |
| **DT.1** | Descrizione del sistema/servizio fornito e dell’Architettura Organizzativa/Logica/funzionale  *È necessario indicare sinteticamente il sistema/servizio fornito comprensivo, nel caso di servizi che utilizzino tecnologia o sistemi informatici, dell’architettura Logico-Funzionale delle infrastrutture tecnologico-informatiche* | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.2** | Elencazione Attrezzature elettromedicali (diagnostiche, strumentali, ecc…) e fornitura di una scheda tecnica per ogni attrezzatura che ne descriva in dettaglio le funzionalità | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.3** | Elencazione e descrizione architetturale dell’infrastruttura HW, (comprensiva di eventuali sistemi esterni alla struttura del Titolare) e di comunicazione (anche di supporto ad attrezzature o per fini di erogazione del servizio)  Indicare analiticamente se l’installazione sia effettuata presso le strutture dell’Azienda (Centro Elaborazione Dati o altra locazione - es. presso Strutture Operative) o presso Strutture Esterne (di proprietà del fornitore o di terzi), indicando la tipologia di infrastruttura prescelta (server fisici o virtuali, hosting, Cloud privato, Cloud pubblico, Cloud ibrido, ecc.…)  Nel caso di installazione presso strutture esterne indicazione se ne sia prevista la collocazione in paesi UE o extra-UE. | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.4** | Elencazione dei sistemi applicativi e middleware utilizzati (es.: software asserviti alle attrezzature, moduli applicativi, sistemi database, web server, ecc…) con indicazione delle relative finalità di utilizzo e architettura generale. (logica o funzionale)  Specificare se siano moduli propri o di terzi (anche in caso di componenti, Web Services o altro) ed il dettaglio dell’architettura sistemistica asservita (n. server fisici/virtuali, middleware utilizzati e relative versioni, DB principali e DB “intermedi” e/o di confine per gestire la comunicazione tra i vari moduli di propria fornitura e/o di terzi). | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.5** | Elenco dei Sistemi di interfaccia/Interfacciamenti con altre piattaforme/moduli software (anche di terzi): per ogni interfaccia indicare i moduli interfacciati dal singolo sistema di interfacciamento e se i dati vengano solo ricevuti, solo inviati o ricevuti ed inviati.  Indicare, per ogni interfacciamento, quali protocolli di comunicazione siano disponibili e quali utilizzati (es.: HL7, DICOM o altro protocollo, se siano utilizzate tecniche di cifratura ed eventualmente quali)  Indicare, per ogni interfacciamento, il dettaglio dei dati conservati (tabelle) e scambiati (messaggistica). | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.6** | Elenco delle Terze parti coinvolte nella fornitura dei prodotti/servizi e del relativo ruolo (es.: erogazione servizi – specificare quali -, manutenzione, produzione attrezzature, produzione di software, hosting, ecc…) e le sedi da cui operano (con indicazione se siano in UE o extra-UE) | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.7** | Elenco, numero e sede delle figure professionali utilizzate nell’erogazione del servizio, e se siano dipendenti, collaboratori o appartenenti a ditte esterne | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.8** | Descrizione se nei sistemi/servizi forniti sia gestito/possibile gestire il ciclo di vita delle informazioni (creazione, uso, trasferimento, dismissione con tempo di conservazione definito); | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.9** | Indicare l’ultima versione rilasciata di ogni singolo modulo software, middleware o asservito all’attrezzatura (elencato nei punti precedenti); | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.10** | Indicare l’ultima versione installata in utilizzo per l’erogazione del servizio di ogni singolo modulo software, middleware o asservito all’attrezzatura (elencato nei punti precedenti); | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.11** | Indicare se l’infrastruttura tecnologica fornita sia basata su sistemi operativi, middleware, altri software o sistemi dichiarati dai produttori “fuori supporto” o non più aggiornati/aggiornabili | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.12** | Indicare nell’infrastruttura tecnologica fornita la presenza di software “embedded” e le modalità di gestione della sicurezza | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.13** | Indicare gli Amministratori di Sistema del servizio/sistema della vostra società e/o di terzi e l’ambito di responsabilità; indicare inoltre le ubicazioni da cui opera tale personale; | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.14** | Indicare le modalità di gestione dei Profili di utenza con indicazione del livello di dettaglio che è possibile raggiungere per le abilitazioni (permessi a livello di modulo, funzionalità, utente o a livello di singolo dato); indicare inoltre se tali utenze siano gestibili tramite protocollo LDAP; | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |
| **DT.15** | Indicare se siano stati forniti i manuali operativi/note di rilascio per l’utilizzo dei servizi/sistemi/prodotti forniti ed i relativi aggiornamenti in caso di upgrade. | * SI * NO | * Descrizione: \_\_\_\_\_\_\_\_\_\_\_\_ * Documento allegato per dettagli (Num. Allegato: \_\_\_\_\_\_\_\_) * Scheda Tecnica (Num. Allegato: \_\_\_\_\_\_\_\_) |

# ELENCO ALLEGATI al presente Accordo

1. ALLEGATO 1 – Ambito di Trattamento
2. ALLEGATO 2 – Principi, Diritti e Misure Tecniche e Organizzative
3. ALLEGATO 3 – Informazioni specifiche sul servizio/prodotto
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
6. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
7. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
8. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
9. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
10. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
11. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
12. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
13. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
14. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
15. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
16. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
17. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
18. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
19. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
20. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
21. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
22. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
23. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
24. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
25. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
26. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
27. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
28. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
29. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
30. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_