Repubblica Italiana

Regione Siciliana

Misure attuative del Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

Informativa sulla protezione dei dati personali per trattamento dati **ai sensi degli artt.13 e 14 del Regolamento UE 2016-679**

InterCUP

Versione 1.0

REPUBBLICA ITALIANA
Regione Siciliana

Informativa sulla protezione dei dati personali
ai sensi degli artt.13 e 14 del Regolamento UE 2016-679

1.Trattamento dei dati personali a cui si riferisce questa informativa
Questa informativa è resa ai sensi degli artt. 13 e 14 del regolamento UE 2016-679 in relazione al Trattamento dati: Navigazione sul portale di accesso ai servizi e coordinamento dei servizi di prenotazione unica della prestazione sanitaria pubblica.
Il servizio attualmente abilitato (INTERCUP) consente la prenotazione, già adesso, con modalità sincrona online oppure, a breve, con modalità alternativa mediante invio di email, che consentirà il rinvio automatico ai sistemi di CUP aziendale del SSR (Sistema Sanitario Regionale)
Il trattamento è improntato rispetto ai principi di correttezza, liceità, pertinenza e trasparenza e tutelando la riservatezza e i diritti dell'interessato ai sensi di legge.

2. Soggetti che intervengono nel trattamento dati
Titolari del trattamento sono le strutture sanitarie

- Azienda Sanitaria Provinciale di Agrigento
- Azienda Sanitaria Provinciale di Caltanissetta
- Azienda Sanitaria Provinciale di Catania
- Azienda Sanitaria Provinciale di Enna
- Azienda Ospedaliera per l'Emergenza Cannizzaro
- Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione Garibaldi
- Azienda Ospedaliero Universitaria Policlinico "G.Rodolico - San Marco"
- Azienda Sanitaria Provinciale di Messina
- Azienda Ospedaliera Papardo di Messina
- A.O.U. Policlinico 'G. Martino' di Messina
- IRCCS Centro Neurolesi Bonino Pulejo
- Azienda Sanitaria Provinciale di Palermo
- Azienda "Civico – Di Cristina – Benfratelli"
- Azienda Ospedaliera Universitaria Policlinico "Paolo Giaccone"
- Azienda Ospedaliera Ospedali Riuniti Villa Sofia Cervello
- Azienda Sanitaria Provinciale di Ragusa
- Azienda Sanitaria Provinciale di Siracusa
- Azienda Sanitaria Provinciale di Trapani

rappresentate dai rispettivi Direttori Generali di cui si riporta sede legale, recapito telefonico e PEC:

RAGIONE SOCIALE	SEDE LEGALE	RECAPITO TELEFONICO	PEC
Azienda Sanitaria Provinciale di Agrigento	Viale della Vittoria, 321 - 92100 Agrigento	0922/407406	protocollo@pec.aspag.it
Azienda Sanitaria Provinciale di Caltanissetta	Via Giacomo Cusmano n°1 - 93100 Caltanissetta	0934/506034	protocollo.asp.cl@pec.asp.cl.it
Azienda Sanitaria Provinciale di Catania	Via S. Maria La Grande 5 - 95124 Catania	095/313859	protocollo@pec.aspct.it
Azienda Sanitaria Provinciale di Enna	Viale A. Diaz, 7 94100, Enna	0935 520111	protocollo.generale@pec.asp.enna.it
Azienda Ospedaliera per l'Emergenza Cannizzaro	Via Messina 829, 95126 Catania	095/7262366	a.o.cannizzaro@pec.it
Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione Garibaldi	Piazza Santa Maria del Gesù 5 - 95124 Catania	095/7593856	protocollo.generale@pec.ao-garibaldi.ct.it
Azienda Ospedaliero Universitaria Policlinico "G.Rodolico - San Marco"	Via S. Sofia, 78 - 95123 Catania	095/3782595	protocollo@pec.policlinico.unict.it
Azienda Sanitaria Provinciale di Messina	Via G. La Farina 263/N - 98124 Messina	090/3652773	protocollogenerale@pec.asp.messina.it
Azienda Ospedaliera Papardo di Messina	Contrada Papardo - 90158 Messina	090/3992916	protocollo@pec-aopapardo.it
A.O.U. Policlinico 'G. Martino' di Messina	Via Consolare Valeria 1 - 98124 Messina	090/3991	protocollo@pec.polime.it
IRCCS Centro Neurolesi Bonino Pulejo	Strada Statale 113 - C.da Casazza - 98124 Messina	090/60128501	azienda@pec.irccsneurolesiboninopulejo.it
Azienda Sanitaria Provinciale di Palermo	Via Giacomo Cusmano n°24 - 90141 Palermo	091/7032336	direzionegenerale@pec.asppalermo.org
Azienda "Civico – Di Cristina – Benfratelli"	Piazza Nicola Leotta 4 - 90127 Palermo	091/6662225	ospedalecivicopa@pec.it
Azienda Ospedaliera Universitaria Policlinico "Paolo Giaccone"	Via del Vespro, 129 90127 Palermo	091/6555204	protocollo@cert.policlinico.pa.it
Azienda Ospedaliera Ospedali Riuniti Villa Sofia Cervello	Viale Strasburgo 233 - 90146 Palermo	091/6802750	protocollo@pec.ospedaliriunitipalermo.it
Azienda Sanitaria Provinciale di Ragusa	Piazza Igea n.1 - 97100 Ragusa	0932/234111	protocollo@pec.asp.rg.it
Azienda Sanitaria Provinciale di Siracusa	Corso Gelone, 17	0931/484321	direzione.generale@pec.asp.sr.it
Azienda Sanitaria Provinciale di Trapani	Via Mazzini 1 - 91100 Trapani	0923/28943	direzione.generale@pec.asptrapani.it

Il Responsabile del trattamento è Almaviva S.p.A., con sede legale in Via di Casal boccone 188/190 00137 Roma.

3. Il Responsabile della protezione dei dati

Il Responsabile della protezione dei dati della Regione Siciliana ha recapito e-mail dpo@regione.sicilia.it e pec dpo@certmail.regione.sicilia.it. Nonché i responsabili delle singole strutture sanitarie:

RAGIONE SOCIALE	EMAIL DPO
Azienda Sanitaria Provinciale di Agrigento	rdp@aspag.it - PEC. rdp@pec.aspag.it
Azienda Sanitaria Provinciale di Caltanissetta	privacy@asp.cl.it
Azienda Sanitaria Provinciale di Catania	patrizia.baiamonte@aspct.it
Azienda Sanitaria Provinciale di Enna	dpo@asp.enna.it
Azienda Ospedaliera per l'Emergenza Cannizzaro	privacy@aoec.it
Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione Garibaldi	privacy@pec.ao-garibaldi.ct.it
Azienda Ospedaliero Universitaria Policlinico "G.Rodolico - San Marco"	privacy@policlinico.unict.it
Azienda Sanitaria Provinciale di Messina	dpo@asp.me.it
Azienda Ospedaliera Papardo di Messina	alessandrapiccolo@aopapardo.it.
A.O.U. Policlinico 'G. Martino' di Messina	dpo@polime.it
IRCCS Centro Neurolesi Bonino Pulejo	alessandra.piccolo@irccsme.it
Azienda Sanitaria Provinciale di Palermo	rpd@asppalermo.org
Azienda "Civico – Di Cristina – Benfratelli"	dpo@arnascivico.it.
Azienda Ospedaliera Universitaria Policlinico "Paolo Giaccone"	dpo@policlinico.pa.it
Azienda Ospedaliera Ospedali Riuniti Villa Sofia Cervello	dpo@ospedaliriunitipalermo.it
Azienda Sanitaria Provinciale di Ragusa	dpo@asp.rg.it
Azienda Sanitaria Provinciale di Siracusa	rpd@asp.sr.it
Azienda Sanitaria Provinciale di Trapani	dpo@pec.asptrapani.it

4.Fonte e Tipologie dei dati personali trattati
I dati personali sono raccolti presso l'interessato per il tramite del sistema di identificazione SPID; i dati di identificazione elettronica per la prestazione sanitaria sono acquisite automaticamente dal sistema Tessera Sanitaria mediante il numero della ricetta elettronica fornito dall'interessato.
I dati personali trattati appartengono alle seguenti categorie:

- dati personali di identificazione dell'assistito acquisiti tramite sistema di autenticazione SPID: codice fiscale nominativo, indirizzo , numeri di telefono, indirizzi e-mail,
- dati della prestazione sanitaria – classificazione categoria particolare dati personali (art.9 GDPR);

5. Finalità e base giuridica del trattamento
La finalità del trattamento è: erogazione del servizio coordinato di prenotazione della prestazione sanitaria presso le strutture sanitarie regionali.
La base giuridica del trattamento è quanto previsto dall'articolo 9 punto h) del Regolamento UE 2016-679. Dalla mancata o parziale comunicazione delle informazioni necessarie potrà derivare la mancata erogazione del servizio.

6. Modalità di trattamento
I dati vengono trattati esclusivamente in relazione alla finalità descritta e con logiche ad essa correlate, con strumenti digitali e telematici, nel rispetto dei principi fissati all'art. 5 del Regolamento (UE) 2016/679, in maniera da garantire un'adeguata sicurezza, compresa la protezione contro trattamenti non autorizzati o illeciti, mediante misure tecniche e organizzative adeguate.
Sulla base dei dati oggetto della presente informativa, non verrà effettuata alcuna profilazione automatizzata.

7. Comunicazione e diffusione dei dati
I dati saranno trattati esclusivamente per le finalità di cui alla presente informativa dai soggetti di cui al punto 2 e dalle persone da loro autorizzate al trattamento.
I dati non saranno comunicati ad altri soggetti.

8. Conservazione dei dati
Per le finalità del trattamento i dati vengono conservati presso le sedi dei Titolari di cui al punto 2 con le modalità e i tempi adottati dai singoli CUP aziendali.
Per le finalità connesse ai servizi INTERCUP i dati vengono anche conservati presso una infrastruttura regionale SPC Cloud Raggruppamento Temporaneo d'imprese Telecom S.p.a. per un periodo di 12 mesi
Qualora i dati siano utilizzati per l'accertamento di responsabilità in caso di ipotetici reati, i termini per la cancellazione sono sospesi a norma di legge.

9. Diritti dell'interessato
L'utente può esercitare i propri diritti di cui agli artt. da 15 a 22 del Regolamento UE 679/2016 sui dati personali che lo riguardano, inviando una comunicazione a ogni singolo Titolare del trattamento presso uno dei recapiti indicati al punto 2, con la quale potrà:

- chiedere conferma o meno sull'esistenza di un trattamento dei propri dati personali;
- chiedere l'accesso agli stessi;
- chiedere la loro rettifica;
- chiedere la cancellazione, fermo restando che tale diritto non si applica per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

- chiedere la limitazione del trattamento;
- opporsi al trattamento;
- chiedere la portabilità dei dati personali, fermo restando che tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

L'interessato potrà in qualsiasi momento proporre reclamo all'Autorità Garante della protezione dei dati personali, piazza Venezia n. 11, scala B, 00187 Roma.

Data 28/01/2021

CENTRO NEUROLESI
BONINO PULEJO
IRCCS MESSINA

IRCCS Centro Neurolesi Bonino Pulejo

Nomina del Responsabile del trattamento dei dati personali relativi all'iniziativa INTERCUP

IL DIRETTORE GENERALE

della Struttura Sanitaria **IRCCS Centro Neurolesi Bonino Pulejo di Messina** di seguito "Struttura", nella qualità di Titolare dei trattamenti dei dati personali specificati in Allegato A

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 che abroga la direttiva 95/46/CE*" e, in particolare, l'art. 27 recante "*Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione*" e l'art. 28 recante "*Responsabile del trattamento*", commi 2 e 4;

Visto il D.lgs. 10 agosto 2018, n. 101 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27-4-2016*";

Visto il D.P. n. 13 del 25/06/2019 con il quale al Dott. Vincenzo Barone è stato conferito l'incarico di Direttore Generale della struttura;

Visto la Deliberazione n. 317 del 26/02/2020 con la quale alla Dott.ssa Alessandra Piccolo è stata conferito l'incarico di "Responsabile della protezione dei dati" per la Struttura;

Visto i Contratti per il Portale di accesso ai servizi e Sovracup stipulati in data 3 ottobre 2019, nell'ambito delle convenzioni Consip "SPC Cloud - lotto 3 e lotto 4", tra l'Autorità Regionale per l'Innovazione Tecnologica e il RTI aggiudicatario dei lotti suddetti, costituito da: Almaviva S.p.A., con sede legale in Via di Casal Boccone, 188/190 - 00137 Roma, Almawave s.r.l., con sede legale in Via di Casal Boccone, 188/190 - 00137 Roma, INDRA ITALIA S.p.A., sede legale in Roma, Via Umberto Saba n.ll, - 00144, PricewaterhouseCoopers Advisory S.p.A., con sede legale in Milano - 20149, Via Monte Rosa n. 91 (nel seguito, "Fornitore");

Considerato che qualora il fornitore sia chiamato ad eseguire le attività di trattamento di dati personali per conto del Titolare, è necessario nominarlo Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27-4-2016, attribuendogli le relative competenze;

Considerato che il fornitore, nella qualità di Responsabile del trattamento dei dati, è obbligato ad adottare le misure di sicurezza di natura fisica, logica, tecnica e organizzativa idonee a

garantire un livello di sicurezza adeguato al rischio e conformi alla normativa vigente indicate dalla Struttura nonché ad attuare le istruzioni fornite dalla Struttura medesima;

Ritenuto quindi, di dover individuare, ai sensi dell'art. 28 del Regolamento UE 2016/679, Almaviva S.p.A. quale Responsabile del trattamento dei dati personali relativi a INTERCUP, come iniziativa specifica nell'ambito dei suddetti Contratti di competenza dell'Autorità regionale per l'Innovazione tecnologica

DECRETA

Art. 1 – Nomina

1. Ai sensi dell'art. 28 del Regolamento UE 2016/679, Almaviva S.p.A. è individuata quale Responsabile del trattamento dei dati personali trattati nell'ambito della suddetta iniziativa INTERCUP.
2. Il Responsabile ha facoltà di designare come Altri Responsabili del trattamento le società o i soggetti subappaltanti, previa informazione scritta al Titolare del trattamento dei dati.
3. Il Responsabile effettua il trattamento dei dati di cui all'allegato "A" al presente provvedimento nei limiti e nel rispetto delle finalità per cui sono trattati. La nomina di Responsabile ha validità dalla data di inizio di operatività del Contratto di cui ai Visti ed è valida fino alla vigenza del Contratto stesso, o fino alla revoca anticipata del presente atto di nomina per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del Contratto o alla revoca, il Responsabile dovrà mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

Art. 2- Obblighi

1. Il Responsabile ha facoltà, nell'ambito dell'esecuzione del Contratto di cui ai Visti, di procedere alla nomina degli autorizzati al trattamento dei dati personali, mediante apposito atto di designazione. Per autorizzato si intende qualsiasi unità di personale interna al Fornitore, che sia autorizzata al trattamento dei dati personali secondo le direttive e istruzioni impartite dal Fornitore stesso. Il Responsabile fornisce alla Struttura l'elenco degli autorizzati.
2. Il Responsabile, nell'ambito dell'esecuzione del Contratto di cui ai Visti, ha l'obbligo di mettere in atto le misure di sicurezza di natura fisica, logica, tecnica e organizzativa indicate dalla Struttura, idonee a garantire un livello di sicurezza adeguato al rischio e conformi alla normativa vigente, tenendo conto delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione.
3. Il Responsabile si deve attenere alle misure di sicurezza indicate dalla Struttura, di cui all'Allegato "B" al presente provvedimento, nonché di quelle specificate nel Contratto di cui ai Visti.
4. Il Responsabile ha l'onere di informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli Altri Responsabili. Il Titolare avrà il diritto di opporsi a tali modifiche, comunicando la propria opposizione per iscritto entro 10 giorni dalla notifica da parte del Responsabile. Il Responsabile non ricorrerà ad Altri Responsabili nei cui confronti il Titolare abbiano manifestato la propria opposizione. Resta inteso che, in mancanza di opposizione, la modifica si intenderà accettata. Il Responsabile impone all'Altro Responsabile con apposito atto gli stessi obblighi in materia di protezione dei dati che sono posti a suo carico in forza del

presente atto e vigila sul loro rispetto. Il Responsabile rimarrà direttamente responsabile nei confronti dei Titolari in ordine alle azioni ed alle omissioni dell'Altro Responsabile e ha l'onere di assicurare che l'Altro Responsabile 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.

Art. 3 - Oneri e Responsabilità

1. Il Responsabile assiste il Titolare in tutte le operazioni relative al trattamento riguardanti il Regolamento UE 2016/679, inclusa quella di fornire risposta alla richiesta di esercizio dei diritti degli interessati.
2. Il Responsabile ha, altresì, l'onere di:
   - **a.** mettere in atto misure tecniche e organizzative al fine di garantire che il trattamento dei dati personali per conto del Titolare sia effettuato in conformità al Regolamento Europeo UE 2016/679;
   - **b.** adottare misure tecniche e organizzative idonee a garantire la sicurezza dei locali e delle postazioni di lavoro;
   - **c.** fornire ai propri dipendenti e collaboratori deputati a trattare i dati personali le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività;
   - **d.** predisporre ed aggiornare sistematicamente il registro delle attività di trattamento dei dati personali trattati per conto del Titolare ed assistere il Titolare nell'aggiornamento del Registro delle categorie di trattamento
   - **e.** cooperare, su richiesta, assieme al Titolare, con l'Autorità garante della protezione dei dati personali (Autorità Garante);
   - **f.** fornire assistenza al Titolare per la gestione del consenso degli interessati al trattamento dei dati personali;
   - **g.** fornire assistenza al Titolare per informare in maniera trasparente gli interessati sulla modalità di gestione e di protezione dei relativi dati personali trattati;
   - **h.** fornire assistenza al Titolare per la gestione delle richieste degli interessati sui propri dati personali trattati per conto del titolare;
   - **i.** fornire assistenza al Titolare per l'analisi del rischio sui dati personali trattati;
   - **j.** fornire assistenza al Titolare per la valutazione d'impatto dell'eventuale uso di nuove tecnologie sulla sicurezza dei dati personali trattati (*data protection impact assessment* o DPIA o VIP);
   - **k.** comunicare al Titolare i dati di contatto del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE 679/2016; il Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione della Struttura;
   - **l.** collaborare con il Titolare e con il Responsabile della protezione dei dati nell'attuazione delle ispezioni interne organizzative e tecniche volte alla verifica dell'attuazione di misure tecniche e organizzative che il Titolare ha definito e di cui ha richiesto l'attuazione;
   - **m.** comunicare i luoghi dove sono memorizzati i dati, le loro copie e i sistemi che trattano i dati, e impegnarsi a non trasferirli in paese terzo rispetto la UE;
   - **n.** fornire assistenza al Titolare nell'aggiornamento della informativa da rendere agli interessati ai sensi degli art. 13 e 14 del Regolamento UE 679/2016 in merito al trattamento in argomento;
   - **o.** rendere disponibili tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dal Regolamento Europeo UE 2016/679;

p. ove risulti che le misure adottate dal Responsabile o dagli Altri Responsabili non siano idonee ad assicurare l'applicazione del Regolamento UE 679/2016 o che non siano correttamente applicate, la Struttura diffiderà il Responsabile ad adottare e far adottare all'Altro Responsabile tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, la Struttura potrà, in ragione della gravità della condotta e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, revocare il presente atto di nomina.

3. Il Responsabile ha l'obbligo di informare il Titolare (inviando una comunicazione a mezzo PEC), senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, di ogni violazione della sicurezza (*data breach*) che occorra nell'ambito delle attività gestite a Contratto dal Responsabile o dagli Altri Responsabili del trattamento per conto del Titolare e 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 ed a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi, sullo stesso gravanti, di notifica delle suddette violazioni all'Autorità Garante ai sensi dell'art. 33 del Regolamento UE 679/2016 o di comunicazione della stessa agli interessati ai sensi dell'art. 34 dello stesso Regolamento. Inoltre il Responsabile comunica le prime misure organizzative e tecniche adottate, relativamente alle attività gestite a Contratto, per porre rimedio alla violazione dei dati personali e per minimizzare gli effetti negativi e propone al Titolare l'adozione di ulteriori misure di sicurezza non immediatamente attuabili. Il Responsabile fornisce al Titolare tutto il necessario supporto e la collaborazione per il riscontro alle richieste di informazioni aggiuntive da parte dell'Autorità Garante.

4. Il Responsabile sarà responsabile per i danni conseguenti a inadempimenti o inosservanze delle istruzioni di cui all'Allegato B al presente provvedimento.

5. Il Responsabile, alla scadenza del Contratto di cui ai Visti o, comunque, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto di nomina, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei dati personali, sarà tenuto ad interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, se richiesto dal Titolare, all'immediata restituzione allo stesso dei dati personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia. Il Responsabile fornisce assicurazione che allo stesso comportamento si sono adeguati gli Altri Responsabili dallo stesso nominati. In caso di richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione dei dati.

Messina,

IL DIRETTORE GENERALE

_____

Allegato A

N.	Denominazione del trattamento	Finalità del trattamento	Categorie di interessati	Categoria dati personali	Durata del trattamento	Responsabile del trattamento	Tempi di conservazione del dato
1	Navigazione sul portale di accesso ai servizi	Prenotazione prestazione sanitaria	Assistiti	Dati personali di identificazione dell'assistito	Fino alla vigenza del contratto	Almaviva	12 mesi
2	Coordinamento dei servizi di prenotazione unica della prestazione sanitaria pubblica	Prenotazione prestazione sanitaria	Assistiti	Dati personali di identificazione dell'assistito Dati della prestazione sanitaria – classificazione categoria particolare dati personali (art.9 GDPR)	Fino alla vigenza del contratto	Almaviva	12 mesi

MISURE DI SICUREZZA

Per garantire la sicurezza dei dati, il Responsabile rivede regolarmente lo stato dell'arte delle tecnologie di sicurezza nell'ambito della propria Organizzazione. Ciò include la determinazione di scenari di danno tipici, le esigenze di sicurezza e i livelli di sicurezza corrispondenti che ne derivano per diversi tipi di dati personali, raggruppati in categorie di possibili danni, nonché l'esecuzione di valutazioni del rischio. Inoltre, vengono effettuati test di penetrazione dedicati per analizzare, esaminare e valutare regolarmente l'efficacia di queste misure tecniche e organizzative che devono garantire la sicurezza del trattamento.

I seguenti aspetti disciplinano l'attuazione di misure tecniche e organizzative appropriate:

1. Backup dei dati

Per evitare perdite, il Responsabile definisce idonee procedure affinché i dati siano regolarmente sottoposti a backup veicolati dalle procedure di sicurezza IT e per la verifica dell'efficacia delle copie di sicurezza.

2. Privacy by design

Il Responsabile garantisce che i principi di protezione/privacy dei dati e di sicurezza dei dati siano presi in considerazione durante i processi di progettazione e sviluppo dei sistemi IT. L'obiettivo è quello di prevenire un'attività di programmazione aggiuntiva, dispendiosa in termini di costi e di tempo, che sarebbe necessaria se i requisiti di privacy e sicurezza dei dati dovessero essere attuati dopo l'installazione dei sistemi IT. All'inizio del processo di sviluppo vengono prese in considerazione misure come la disattivazione di alcune funzionalità software, l'autenticazione, la pseudonimizzazione o la crittografia.

Il Responsabile esterno si assicura che siano trattati solo i dati personali necessari per il relativo scopo.

In particolare va assicurato il ricorso alla pseudonimizzazione dei dati in tutti i casi in cui non sia possibile o sostenibile cifrarli.

Inoltre il Responsabile dovrà mettere in atto tutte le misure tecniche ed organizzative al fine di assicurare:

- la riservatezza, l'integrità, la disponibilità dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente tecnico;
- la verifica e la valutazione periodica dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Comunicazioni via e-mail

Considerato che il contenuto delle e-mail può essere visualizzato anche da terzi, le comunicazioni relative ad informazioni riservate non devono essere effettuate per e-mail non crittografate, quando la riservatezza delle informazioni trasmesse non può essere garantita.

4. Amministrazione da remoto

Nel caso i dipendenti o subappaltatori del Responsabile debbano accedere ai dati dei soggetti istanti o del titolare, l'accesso è disciplinato dalle seguenti regole generali:

- l'accesso all'amministrazione da remoto è chiuso per impostazione predefinita e viene autorizzato solo dall'Amministratore di sistema, il quale avrà la possibilità di monitorare gli interventi;

• le password per accedere ai sistemi IT vengono rilasciate dall'Amministratore di sistema solo per le finalità di cui all'Allegato A;

• gli interventi critici sono garantiti da una procedura "4-eyes" (principio del doppio controllo);

• l'accesso all'amministrazione da remoto viene registrato nel sistema. Vengono registrati i seguenti dati: persona responsabile, data e ora, durata, sistema di destinazione, breve descrizione dell'attività svolta e, in caso di interventi critici, i nominativi del personale qualificato aggiuntivo consultato nell'applicazione della procedura "4-eyes";

• la registrazione delle sessioni di amministrazione da remoto è vietata, salvo i casi in cui sia necessaria per la risoluzione dei problemi segnalati dal Titolare.

5. Misure di sicurezza IT

Il Responsabile, in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 e nella qualità di Amministratore di sistema si adegua a quanto prescritto dal Provvedimento del Garante della privacy del 27/11/2008 ed in particolare cura:

• la valutazione delle caratteristiche soggettive nell'attribuzione della funzione di amministratore di sistema o applicativo;

• la designazione individuale dell'amministratore di sistema o applicativo con elencazione analitica degli ambiti di operabilità;

• l'elenco degli amministratori di sistema o applicativi

• la conservazione degli estremi delle persone preposte quali amministratori di sistema o applicativi;

• la verifica delle attività degli amministratori di sistema o applicativi almeno con cadenza annuale;

• la registrazione degli accessi logici agli archivi elettronici in elenchi aventi le caratteristiche di completezza; inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste dovranno essere garantite dall'infrastruttura. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate.

6. Protezione Antivirus

Ogni postazione di lavoro del Responsabile è protetta da sistemi di sicurezza contro le minacce informatiche (antivirus) e ne è consentito l'utilizzo unicamente mediante appositi sistemi di autenticazione e profilazione.

7. Altre misure

• Garantire che le connessioni siano effettuate esclusivamente tramite protocollo HTTPS

• Incrementare la consapevolezza dei soggetti autorizzati attraverso una serie di misure che implicano formazione, aggiornamento e accesso a procedure e *policy* specifiche in ambito *privacy* e *security*, prevedendo contemporaneamente l'attribuzione di responsabilità specifiche e possibili provvedimenti in caso di mancato rispetto delle stesse o delle policy

• Adottare opportune politiche per la gestione di eventuali casi di *data breach*

• Per le utenze gestite e in carico al Responsabile, attuare una gestione degli account utenti che consideri il ciclo di vita dell'account, dalla creazione alla dismissione dello stesso, prevedendo anche una procedura di revisione periodica

- Gestire i log di accesso e gli eventuali accessi non autorizzati, impostando delle procedure specifiche per entrambe le situazioni, fornendo una debita informativa al Titolare.