

REPUBBLICA ITALIANA  
REGIONE SICILIANA



ASSESSORATO SALUTE  
Dipartimento Attività Sanitarie ed Osservatorio epidemiologico

**Nomina del Responsabile esterno del trattamento dei dati personali relativi alla gestione del programma di accreditamento dei provider ECM regionali**

**IL DIRIGENTE GENERALE**

- Visto** lo Statuto della Regione siciliana;
- Viste** la Legge regionale 29 dicembre 1962, n. 28 e la Legge regionale 10 aprile 1978, n. 2;
- Vista** la Legge regionale 8 luglio 1977, n. 47 recante “*Norme in materia di bilancio e contabilità della Regione Siciliana*”;
- Vista** la Legge Regionale 12 agosto 2014, art. 68, comma 4 inerente l’obbligo di pubblicazione dei decreti assessoriali sul sito internet della Regione Siciliana;
- 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*”;
- Vista** la deliberazione della Giunta regionale di Governo 28 maggio 2018, n. 203 “*Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27-4-2016 – nomina del Responsabile per la protezione dei dati*”;
- Vista** la deliberazione della Giunta Regionale di Governo 29 novembre 2018 n. 483, recante “*Regolamento UE 2016/679 – Adozione delle prime istruzioni organizzative e tecniche per il trattamento dei dati personali, di una procedura di risposta e di un questionario di autovalutazione*”
- Visto** il D.P.Reg. n. 777/AREA 1/S.G. del 15/11/2022 con il quale il Presidente della Regione ha nominato la D.ssa Giovanna Volo Assessore regionale con preposizione all’Assessorato regionale della Salute;
- Visto** il D.P.R.S. 12 giugno 2018, n. 569 con il quale è stato nominato “*Responsabile della protezione dei dati*” per la Regione Siciliana;
- Visto** il D.P. Reg. n. 5687 del 22 dicembre 2022 con il quale, in esecuzione della deliberazione della Giunta regionale n. 586 del 16 dicembre 2022, al Dott. Salvatore Requirez, è stato

conferito, l'incarico di Dirigente Generale del Dipartimento Attività sanitarie ed osservatorio epidemiologico dell'Assessorato regionale della Salute;

**Visto** il D.A. del 31/01/2023, n.8 con il quale l'Assessore della Salute, nella qualità di Titolare del trattamento, ha conferito al Dirigente generale del suddetto dipartimento regionale, l'incarico di Responsabile dei trattamenti di dati personali che rientrano tra le competenze del Dipartimento Attività Sanitarie ed Osservatorio Epidemiologico con facoltà di ricorrere ad altri soggetti responsabili ai quali affidare in tutto o in parte il trattamento dei dati, ai sensi dell'art. 28 del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;

**Visto** il D.D.G. n. 2103 del 12 novembre 2018 con il quale è stata approvata la Procedura per l'accreditamento standard dei provider ECM della Regione Siciliana

**Considerato** che è in atto di stipula la convenzione tra la Regione Sicilia nella persona del Dirigente Generale del DASOE e l'Agenas (Agenzia nazionale per i Servizi Sanitari) per l'affidamento da parte della Regione Siciliana all'Agenas di attività operative, procedurali e informatiche finalizzate al supporto per la realizzazione e la gestione del programma di accreditamento dei provider Ecm regionali .

**Considerato** che qualora il fornitore sia chiamato ad eseguire le attività di trattamento di dati personali per conto del Titolare, è necessario nominarlo Responsabile esterno 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 esterno del trattamento dei dati, sia 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 e alle istruzioni fornite dall'Amministrazione;

**Ritenuto** quindi, di dover individuare, ai sensi dell'art. 28 del Regolamento UE 2016/679, l'Agenas C.F. 97113690586 con sede legale in Roma in Via Puglie, 23 quale Responsabile esterno del trattamento dei dati personali relativi alla gestione del programma di accreditamento dei provider ECM regionali di competenza dell'Assessorato regionale della Salute - DASOE;

## **DECRETA**

### **Art. 1 – Nomina**

- 1.** Ai sensi dell'art. 28 del Regolamento UE 2016/679, l'AGENAS con sede legale in ROMA Via Puglie, 23 C.F. 97113690586 è individuata quale Responsabile esterno del trattamento dei dati personali relativi alla gestione del programma di accreditamento dei provider ECM regionali relativamente alla Convenzione in itinere tra il Dirigente generale del DASOE e la Società stessa.
- 2.** Il Responsabile esterno effettua il trattamento dei dati per le attività di cui alla convenzione in atto di stipula. La nomina di Responsabile esterno ha validità dalla data di inizio operatività della convenzione di cui al comma 1 del presente articolo ed è valida fino alla vigenza della stessa, o fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del Convenzione o alla revoca, il Responsabile

esterno 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 esterno ha facoltà, nell'ambito dell'esecuzione della Convenzione di cui all'art.1, 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 alla Società, che sia autorizzata al trattamento dei dati personali secondo le direttive e istruzioni impartite dalla Società stessa. Il Responsabile esterno fornisce, all'Assessorato della Salute l'elenco degli autorizzati.
2. Il Responsabile esterno, nell'ambito dell'esecuzione del contratto di cui all'art. 1, ha l'obbligo di mettere in atto 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, 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 esterno si deve attenere alle misure di sicurezza indicate dall'Assessorato regionale - DASOE, di cui all'Allegato "B" al presente provvedimento, nonché di quelle specificate nel Contratto di cui all'art. 1 e nei relativi allegati.
4. Il Responsabile esterno ha l'onere di informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli ulteriori sub-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 esterno. Il Responsabile esterno non ricorrerà ai sub-Responsabili nei cui confronti il Titolare abbia manifestato la propria opposizione. Resta inteso che, in mancanza di opposizione, la modifica si intenderà accettata. Il Responsabile esterno impone al sub-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 esterno rimarrà direttamente responsabile nei confronti del Titolare in ordine alle azioni ed alle omissioni dei propri sub-Responsabili ed ha l'onere di assicurare che il sub-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 esterno assiste il Titolare in tutte le operazioni di sua competenza, inclusa quella di fornire risposta alla richiesta di esercizio dei diritti degli interessati, e ha l'onere di svolgere compiti di direzione e coordinamento sul corretto trattamento dei dati personali.
2. Il Responsabile esterno ha, altresì, l'onere di:
  - a. mettere in atto misure tecniche e organizzative atte a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali per conto del Titolare è 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 suo Registro delle categorie di trattamento e il DASOE dell'Assessorato della Salute nell'aggiornamento del Registro delle categorie di attività di trattamento ;
  - e. cooperare, su richiesta, assieme al Titolare, con l'Autorità garante della protezione dei dati personali (Autorità Garante) nell'esecuzione dei suoi compiti;
  - 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 le 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 esterno collabora e si tiene in costante contatto con il Responsabile della protezione dei dati della Regione Siciliana.
  - l. collaborare con il Titolare e con il Responsabile della protezione dei dati della Regione Siciliana nell'attuazione delle ispezioni interne organizzative e tecniche volte alla verifica dell'attuazione di misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 2016/679;
  - m. comunicare i luoghi dove sono memorizzati i dati, le loro copie e i sistemi che li trattano, 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 da un sub-Responsabile non siano idonee ad assicurare l'applicazione del Regolamento UE 679/2016 o che siano non siano correttamente applicate, l'Amministrazione diffiderà il Responsabile ad adottare e far adottare al sub-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, l'Amministrazione potrà, in ragione della gravità della condotta e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il Contratto di cui all'art.1 con il Responsabile esterno ed escutere la garanzia l'eventuale garanzia prestata, salvo il risarcimento del maggior danno.
3. Il Responsabile esterno 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 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 comunica le prime misure organizzative e tecniche adottate 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 esterno 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 esterno sarà responsabile per i danni conseguenti a inadempimenti o inosservanze delle istruzioni di cui all'Allegato B al presente provvedimento o di quelle successive eventualmente trasmesse per iscritto dall'Assessorato regionale della salute
5. Il Responsabile esterno, alla scadenza della convenzione di cui all'art.1 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, a scelta del 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 esterno non ne esiste alcuna copia. Il Responsabile esterno fornisce assicurazione che allo stesso comportamento si sono adeguati i sub-Responsabili dallo stesso nominati. In caso di richiesta scritta del Titolare, il Responsabile esterno è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione dei dati.

Il presente decreto sarà pubblicato in forma integrale nella Gazzetta Ufficiale della Regione Siciliana e sul sito web dell'Assessorato Regionale della Salute- DASOE.

Palermo, 03/07/2023

IL DIRIGENTE GENERALE

---

## **MISURE DI SICUREZZA**

Per garantire la sicurezza dei dati, il Responsabile esterno rivede regolarmente lo stato dell'arte delle tecnologie di sicurezza. 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 esterno definisce idonee procedure affinché i dati vengono 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 esterno 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 esterno dovrà mettere in atto tutte le misure tecniche ed organizzative al fine di assicurare:

- la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o 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 esterno 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, il quale avrà la possibilità di monitorare gli interventi;

- le password per accedere ai sistemi IT vengono rilasciate dall'Amministratore solo per le finalità di cui all'Allegato A;
- gli interventi critici sono garantiti da una procedura "4-eyes" (principio del doppio controllo) con ulteriore presenza dell'interessato;
- 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 esterno rispetta delle "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni", emanate dall'AgID con circolare n. 2/2017 del 18 aprile 2017 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 gli 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. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore ai 6 mesi.

## **6. Firewall o sicurezza perimetrale**

Le reti informatiche del Responsabile esterno devono essere protette da sistemi di sicurezza perimetrale (c.d. Firewall) e da altre apparecchiature all'uopo destinate mantenute aggiornate allo stato dell'arte.

## **7. Protezione Antivirus**

Ogni postazione di lavoro del Responsabile esterno 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.

## **8. Altre misure**

- Adottare opportune politiche di *data recovery* e *business continuity*
- 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*
- 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 e, nel caso, all'Autorità Garante