DELIBERAZIONE DELLA GIUNTA REGIONALE 7 ottobre 2025, n. 1398

Aggiornamento delle disposizioni procedurali per la compilazione del Registro delle Attività di Trattamento dati personali (R.A.T.) della Regione Puglia ex art. 30 Reg. UE 679/2016 (GDPR) e adozione del Registro delle Violazioni, integrato all'interno del R.A.T. - Modifiche ed integrazioni alla D.G.R. n. 2159 del 2021.

LA GIUNTA REGIONALE

VISTI:

- gli artt. 4, 5 e 6 della L.R. 4 febbraio 1997, n. 7;
- la Deliberazione della Giunta Regionale n. 3261 del 28 luglio 1998;
- gli artt. 4 e 16 del D.lgs. n. 165 del 30.03.2001 e ss.mm.ii.;
- gli artt. 43 e 44 dello Statuto della Regione Puglia;
- il Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii., recante l'Atto di Alta Organizzazione "M.A.I.A. 2.0";
- il Regolamento interno di questa Giunta;

VISTO il documento istruttorio della Sezione Affari Istituzionali e Giuridici, concernente l'argomento in oggetto e la conseguente proposta del Presidente della Giunta regionale;

PRESO ATTO

a) delle sottoscrizioni dei responsabili della struttura amministrativa competente, ai fini dell'attestazione della regolarità amministrativa dell'attività istruttoria e della proposta, ai sensi dell'art. 6, co. 8 delle Linee guida sul "Sistema dei controlli interni nella Regione Puglia", adottate con D.G.R. 23 luglio 2019, n. 1374;
b) della dichiarazione del Segretario Generale della Presidenza, in merito a eventuali osservazioni sulla proposta di deliberazione, ai sensi degli artt. 18 e 20 del Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii.

Con voto favorevole espresso all'unanimità dei presenti e per le motivazioni contenute nel documento istruttorio che è parte integrante e sostanziale della presente deliberazione

DELIBERA

1. di procedere all'aggiornamento delle disposizioni procedurali per la compilazione del Registro delle Attività di Trattamento (R.A.T.) della Regione Puglia contenute nella DGR n. 2159/2021, adeguandole alle revisioni ed integrazioni intervenute nel tempo;
2. di adottare il Registro delle Violazioni della Regione Puglia in formato digitale - in sostituzione del registro cartaceo delle violazioni dei dati personali di cui alla DGR. n. 1905/2022 - che sarà reso disponibile nella relativa Sezione "Registro Violazioni" dell'applicativo informatico per la tenuta del Registro delle Attività di Trattamento (R.A.T.), accessibile tramite l'indirizzo web https://gdpr.regione.puglia.it;
3. di dare atto che al fine di annotare in un unico archivio anche le violazioni dei dati personali temporalmente antecedenti all'adozione del Registro delle Violazioni in formato digitale, la registrazione delle informazioni contenute nel precedente registro cartaceo verranno fatte confluire d'ufficio nel Registro delle Violazioni digitale;
4. di approvare, conseguentemente, la "Guida alla compilazione del Registro delle Attività di Trattamento dati personali (R.A.T.) e dell'integrato Registro delle Violazioni della Regione Puglia", Allegato A) al presente provvedimento per farne parte integrante e sostanziale, che sostituisce la "Guida alla compilazione del Registro delle Attività di Trattamento (R.A.T.) della Regione Puglia", Allegato A) alla DGR n. 2159/2021;

5. di pubblicare il presente provvedimento in versione integrale sul Bollettino Ufficiale della Regione Puglia ai sensi della L.R. n. 18/2023 s.m.i.;
6. di demandare alla Sezione Affari Istituzionali e Giuridici la trasmissione del presente provvedimento ai Direttori di Dipartimento, ai Dirigenti di Sezione e Servizio della Regione Puglia per gli adempimenti conseguenti;
7. di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 12 del decreto legislativo 14 marzo 2013, n. 33 e, per l'effetto, di pubblicare il presente provvedimento sul Portale istituzionale regionale all'interno della Sezione "Amministrazione trasparente", Sottosezione "Disposizioni Generali/Atti generali/Atti amministrativi Generali".

Il Segretario Generale della Giunta
NICOLA PALADINO

Il Presidente della Giunta
MICHELE EMILIANO

DOCUMENTO ISTRUTTORIO

Oggetto: Aggiornamento delle disposizioni procedurali per la compilazione del Registro delle Attività di Trattamento dati personali (R.A.T.) della Regione Puglia ex art. 30 Reg. UE 679/2016 (GDPR) e adozione del Registro delle Violazioni, integrato all'interno del R.A.T. – Modifiche ed integrazioni alla D.G.R. n. 2159 del 2021.

Visti:

- La Deliberazione della Giunta Regionale 7 dicembre 2020, n. 1974, recante approvazione del nuovo Modello Organizzativo regionale "MAIA 2.0" e successive modifiche e integrazioni;
- Il Decreto del Presidente della Giunta Regionale 22 gennaio 2021, n. 22, recante adozione dell'Atto di alta organizzazione connesso al suddetto Modello organizzativo "MAIA 2.0" e successive modifiche e integrazioni;
- La Deliberazione della Giunta Regionale 26 aprile 2021, n. 676, con la quale è stato conferito l'incarico di Segretario Generale della Presidenza, prorogato con successivi atti, da ultimo con Delibera di Giunta Regionale n. 637 del 21 maggio 2025;
- La Deliberazione della Giunta Regionale 4 novembre 2019, n. 1930, con la quale è stato conferito l'incarico di direzione della Sezione Affari istituzionali e Giuridici, prorogato con Deliberazione di Giunta Regionale del 28 ottobre 2022 n. 1478 e, da ultimo, con Delibera di Giunta Regionale 27 giugno 2025 n. 918;
- La Deliberazione della Giunta Regionale 9 dicembre 2019 n. 2297, con la quale è stato designato il *Data Protection Officer* (DPO) della Regione Puglia;
- La Deliberazione della Giunta Regionale 15 settembre 2021, n. 1466, recante l'approvazione della Strategia regionale per la parità di genere, denominata "Agenda di Genere";
- La Deliberazione della Giunta Regionale 26 settembre 2024, n. 1295, recante "Valutazione di impatto di genere (VIG). Approvazione indirizzi metodologico-operativo e avvio fase strutturale";
- Il Regolamento (UE) n. 679/2016 – GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Il D.Lgs. n.196/2003 s.m.i. recante "Codice in materia di protezione dei dati personali";
- La Deliberazione della Giunta Regionale 22 dicembre 2021 n. 2159 recante *"Registro informatico delle Attività di Trattamento dati personali della Regione Puglia ex art. 30 Reg. UE 679/2016 (GDPR) – Disposizioni procedurali per la compilazione"*;
- La Deliberazione della Giunta Regionale 19 dicembre 2022 n. 1905 *recante "Procedura per la gestione degli eventi di violazione dei dati personali (c.d. Data Breach) ai sensi degli artt. 33 e 34 Regolamento UE 2016/679 (GDPR). Adozione".*

Premesso che:

- Il Regolamento (UE) 2016/679 ("*General Data Protection Regulation*", d'ora innanzi GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato essenzialmente sulla valutazione dei rischi inerenti i diritti e le libertà degli interessati, ha riformato il precedente impianto normativo nazionale in materia di protezione dei dati personali (D.Lgs. 196/2003, cd. "Codice Privacy"), inserendo come elemento cardine il principio di "*accountability*" ("responsabilizzazione") posto in capo al Titolare del trattamento, nonché ad eventuali Responsabili, i quali sono tenuti a garantire la conformità al GDPR di tutte le attività di trattamento dati e la tutela dei diritti dell'interessato attraverso l'adozione di misure tecniche ed organizzative adeguate ed efficaci, sottoposte a continuo aggiornamento;
- Il D.Lgs. 101/2018 ha introdotto disposizioni per l'adeguamento del D.Lgs. n. 196/2003 "Codice Privacy" alle disposizioni del sopraccennato GDPR;
- Il GDPR detta una complessa disciplina di carattere generale, prevedendo molteplici obblighi e adempimenti in capo ai soggetti che trattano dati personali ed attribuendo, al tempo stesso, al Titolare del trattamento il compito di individuare le modalità operative per porre in essere i prescritti adempimenti;
- Una delle misure fondamentali poste a carico del Titolare o di suoi delegati, e degli eventuali Responsabili o loro delegati, per dare conto delle attività di trattamento svolte e delle misure messe in atto ai fini della protezione dei dati personali, è il Registro delle Attività di Trattamento previsto dall'art. 30 del GDPR;
- Fra gli adempimenti di maggiore rilevanza ci sono anche quelli connessi alla gestione di eventuali violazioni di dati personali (cd. *data-breach*), ossia a qualsiasi "*violazione di 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*", ai sensi degli artt. 33 e 34 del GDPR, a mente dei quali il Titolare è tenuto alla notifica all'Autorità di Controllo (Garante per la protezione dei dati personali) senza ingiustificato ritardo – e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza – di ogni violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche;
- In caso di violazione, in base al richiamato art. 33 GDPR, par. 5, il Titolare del trattamento è altresì tenuto a *"documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*, all'interno di apposito Registro delle violazioni;

- Dal punto di vista soggettivo, con D.G.R. n. 145 del 30/1/2019 la Giunta Regionale della Puglia, in applicazione del disposto dell'art. 2-quaterdecies del D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679", ha delegato l'esercizio delle competenze del Titolare del trattamento in materia di protezione dei dati ai Dirigenti responsabili delle singole Strutture presso le quali si svolgono i trattamenti di dati specifici, nominando questi ultimi "Designati al trattamento dei dati" e segnatamente definendone i relativi compiti. Tra i compiti dei Designati al trattamento figurano l'aggiornamento e l'implementazione - per quanto di propria competenza e nell'ambito delle proprie funzioni - del Registro delle Attività di Trattamento (R.A.T.) svolte per conto del Titolare e la gestione degli eventi di *data breach*;
- Con D.G.R. n. 2159/2021 la Giunta Regionale, in attuazione dell'art. 30 del GDPR innanzi citato, ha proceduto ad approvare la "Guida alla compilazione del Registro delle Attività di Trattamento (R.A.T.) della Regione Puglia", Allegato A) al medesimo provvedimento, al fine di fornire indicazioni operative di dettaglio che supportino i Dirigenti, nella loro qualità di Designati al trattamento *ex* DGR 145/2019, o i soggetti da essi autorizzati, nella corretta gestione del R.A.T. e, segnatamente, al fine di garantire modalità uniformi di compilazione e tenuta a livello regionale dello stesso Registro;
- Con D.G.R. 1905/2022 la Giunta Regionale ha approvato inoltre, in applicazione dei citati artt. 33 e 34 del GDPR, la "Procedura per la gestione degli eventi di violazione dei dati personali (cd. *data breach*) della Regione Puglia", unitamente al relativo Registro delle violazioni di dati personali in formato cartaceo.

Considerato che:

- Negli ultimi anni, successivamente all'approvazione delle disposizioni procedurali di cui alla succitata DGR n. 2159/2021, la struttura del Registro delle Attività di Trattamento (R.A.T.) è stata oggetto di alcune revisioni, integrazioni ed aggiornamenti al fine di razionalizzare e completare le informazioni disponibili all'interno dello stesso Registro.
- Inoltre con la cennata D.G.R. 1905/2022, recante "Procedura per la gestione degli eventi di violazione dei dati personali (cd. *data breach*) della Regione Puglia", la Giunta Regionale aveva disposto, tra l'altro, che anche per il Registro delle violazioni si dovesse procedere, nel triennio 2023-2025, alla progettazione e messa a regime di un software applicativo regionale dedicato.
- Il menzionato R.A.T. si è arricchito nello specifico, nel corso del tempo, delle seguenti implementazioni:

a) un nuovo collegamento nella *Home Page* del Portale, dal quale risulta scaricabile l'Informativa Privacy afferente allo stesso Registro delle Attività di Trattamento Dati (R.A.T.) della Regione Puglia;
b) una nuova colonna, denominata "Esito controlli", presente nella pagina relativa all'elenco dei trattamenti censiti da ciascuna Struttura designata, che dà conto della completezza o meno della compilazione di tutte le sezioni del RAT o, in alternativa, dell'avvenuta conclusione/cessazione del trattamento;
c) una nuova pagina all'interno della Sezione Dati Generali, che consente di collegare un unico trattamento di dati (che presenti base giuridica, finalità, dati personali trattati e modalità di trattamento analoghe) a più procedimenti amministrativi - censiti dalle Strutture della Giunta Regionale nel Catalogo dei Procedimenti, pubblicato nella Sezione "Amministrazione Trasparente" del Portale regionale;
d) una nuova Pagina dedicata all'individuazione di eventuali Responsabili Esterni, con l'aggiunta del campo "Sub-Responsabili Esterni" del trattamento;
e) una nuova Sezione *ad hoc* dedicata all'individuazione di eventuali Contitolari del trattamento: tale informazione, nel precedente assetto del R.A.T., era interna alla Sezione "Dati Generali";
f) una nuova impostazione della Sezione "Trasferimenti", che consente preventivamente di indicare la presenza o meno di dati personali trasferiti verso un Paese Terzo o una Organizzazione Internazionale;
g) la possibilità di inserire nelle Sezioni dedicate ad "Analisi dei Rischi" e "DPIA" una pluralità di documenti/report (*files*), al fine di tenere traccia di tutti gli aggiornamenti nel tempo di Valutazioni di Impatto-DPIA ed Analisi Rischi rispetto ad uno specifico trattamento di dati personali;
h) una nuova Sezione relativa al "Registro Violazioni", corredata di schede di dettaglio (Categoria di soggetti coinvolti, Categoria di dati violati, Misure di sicurezza adottate, Allegati) inerenti le eventuali violazioni che abbiamo interessato lo specifico trattamento di dati personali censito nel RAT.

Per quanto innanzi si è ritenuto opportuno formulare un aggiornamento della Guida alla compilazione del RAT approvata con DGR n. 2159/2021, che tenga conto di tutte le implementazioni effettuate nel tempo, ivi compresa l'adozione del Registro delle Violazioni in formato digitale quale Sezione del R.A.T.

Garanzie di riservatezza

La pubblicazione sul BURP, nonché la pubblicazione all'Albo o sul sito istituzionale, salve le garanzie previste dalla legge 241/1990 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 2016/679 in materia di protezione dei dati personali, nonché dal D.Lgs. 196/2003 ss.mm.ii., ed ai sensi del vigente Regolamento regionale 5/2006 per il trattamento dei dati sensibili e giudiziari, in quanto applicabile. Ai fini della pubblicità legale, il presente provvedimento è stato redatto in modo da evitare la diffusione di dati personali identificativi non necessari ovvero il riferimento alle particolari categorie di dati previste dagli articoli 9 e 10 del succitato Regolamento UE.

Esiti Valutazione di impatto di genere: neutro

COPERTURA FINANZIARIA AI SENSI DEL D.LGS. 118/2011 E SS.MM.II.

Il presente provvedimento non comporta implicazioni, dirette e/o indirette, di natura economico-finanziaria e/o patrimoniale e dalla stessa non deriva alcun onere a carico del bilancio regionale.

Tutto ciò premesso, al fine dell'adozione del conseguente atto finale, ai sensi dell'art. 4, co. 4, lett. d,) della L.R. 7/1997, si propone alla Giunta regionale:

1. di procedere all'aggiornamento delle disposizioni procedurali per la compilazione del Registro delle Attività di Trattamento (R.A.T.) della Regione Puglia contenute nella DGR n. 2159/2021, adeguandole alle revisioni ed integrazioni intervenute nel tempo;
2. di adottare il Registro delle Violazioni della Regione Puglia in formato digitale - in sostituzione del registro cartaceo delle violazioni dei dati personali di cui alla DGR. n. 1905/2022 - che sarà reso disponibile nella relativa Sezione "Registro Violazioni" dell'applicativo informatico per la tenuta del Registro delle Attività di Trattamento (R.A.T.), accessibile tramite l'indirizzo web https://gdpr.regione.puglia.it;
3. di dare atto che al fine di annotare in un unico archivio anche le violazioni dei dati personali temporalmente antecedenti all'adozione del Registro delle Violazioni in formato digitale, la registrazione delle informazioni contenute nel precedente registro cartaceo verranno fatte confluire d'ufficio nel Registro delle Violazioni digitale;
4. di approvare, conseguentemente, la "Guida alla compilazione del Registro delle Attività di Trattamento dati personali (R.A.T.) e dell'integrato Registro delle Violazioni della Regione Puglia", Allegato A) al presente provvedimento per farne parte integrante e sostanziale, che sostituisce la "Guida alla compilazione del Registro delle Attività di Trattamento (R.A.T.) della Regione Puglia", Allegato A) alla DGR n. 2159/2021;
5. di pubblicare il presente provvedimento in versione integrale sul Bollettino Ufficiale della Regione Puglia ai sensi della L.R. n. 18/2023 s.m.i.;
6. di demandare alla Sezione Affari Istituzionali e Giuridici la trasmissione del presente provvedimento ai Direttori di Dipartimento, ai Dirigenti di Sezione e Servizio della Regione Puglia per gli adempimenti conseguenti;
7. di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 12 del decreto legislativo 14 marzo 2013, n. 33 e, per l'effetto, di pubblicare il presente provvedimento sul Portale istituzionale regionale all'interno della Sezione "Amministrazione trasparente", Sottosezione "Disposizioni Generali/Atti generali/Atti amministrativi Generali".

I sottoscritti attestano la regolarità amministrativa dell'attività istruttoria e della proposta, ai sensi dell'art. 6, co. 3, lett. da *a)* ad *e)* delle Linee guida sul "Sistema dei controlli interni nella Regione Puglia", adottate con D.G.R. 23 luglio 2019, n. 1374.

Il Responsabile E.Q.
"Protezione dei dati personali
nel sistema Regione": Gianvito Giordano

Gianvito Giordano
05.09.2025
13:24:57
GMT+02:00

Il Responsabile E.Q.
"Audit privacy e
sistemi informativi": Maria Lucatorto

Maria Lucatorto
05.09.2025
13:29:48
GMT+02:00

IL DIRIGENTE della Sezione
"Affari Istituzionali e Giuridici": Rossella Caccavo

Rossella Caccavo
05.09.2025 14:03:52
GMT+02:00

Il Segretario Generale della Presidenza ai sensi degli artt. 18 e 20 del Decreto del Presidente della Giunta regionale 22 gennaio 2021, n. 22 e ss.mm.ii., NON RAVVISA la necessità di esprimere osservazioni a quanto riportato nell'allegato A alla presente proposta di DGR.

Il Segretario Generale della Presidenza: Roberto Venneri

ROBERTO
VENNERI

Il Presidente della Giunta Regionale, dott. Michele Emiliano, ai sensi del vigente Regolamento della Giunta regionale,

propone

alla Giunta regionale l'adozione del presente atto.

Michele
Emiliano
24.09.2025
16:06:11
GMT+02:00

Allegato A

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DATI PERSONALI (R.A.T.) E REGISTRO DELLE VIOLAZIONI DELLA REGIONE PUGLIA

– GUIDA ALLA COMPILAZIONE –

Sommario

1. Premessa

Il Registro delle Attività di Trattamento di dati personali (R.A.T.) è previsto dall'art. 30 (C. 82) del Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR) come misura fondamentale a carico del Titolare del trattamento o suoi delegati, nonché del Responsabile del trattamento o suoi delegati, per rendere conto dell'attività e delle misure messe in atto ai fini della protezione dei dati personali gestiti nell'ambito della propria organizzazione.

Nell'ambito della Regione Puglia il Titolare del trattamento, con D.G.R. n. 145/2019, ha individuato quali Designati al trattamento tutti i dirigenti regionali, cui l'art. 4 dell'Allegato A) al predetto atto deliberativo conferisce, fra l'altro, funzioni di gestione – *ratione materiae* – del Registro delle attività di trattamento: ciascun dirigente regionale, in qualità di Designato, provvede pertanto direttamente alla tenuta e all'aggiornamento del Registro, potendo farsi supportare nelle attività di compilazione del Registro da tutti i soggetti da lui espressamente nominati quali "Autorizzati" al trattamento dei dati gestiti dalla struttura organizzativa di riferimento.

La finalità del presente documento è quella di fornire indicazioni operative di dettaglio che supportino i Dirigenti, nella loro qualità di Designati al trattamento ex DGR 145/2019, o i soggetti da essi autorizzati, nella corretta gestione del Registro delle attività di trattamento, tenuto in formato elettronico ed accessibile all'indirizzo web https://gdpr.regione.puglia.it, secondo quanto previsto dal GDPR.

Si ritiene utile precisare inoltre, in via preliminare, che la Regione Puglia può agire – a seconda delle caratteristiche del trattamento dati in questione – come Titolare o come Responsabile del trattamento, a seconda che definisca o meno le finalità e i mezzi del trattamento di dati. Ovviamente la seconda fattispecie è solo residuale. Il Registro delle Attività di Trattamento dati della Regione Puglia, tenuto in formato elettronico, consente di inserire tutti i trattamenti di dati effettuati dalla Regione, tanto nell'ipotesi (principale) che la Regione sia Titolare del trattamento quanto nell'ipotesi (residuale) in cui essa agisca quale Responsabile del trattamento (cfr., rispettivamente, par. 5 e 7 della presente Guida).

Inoltre, in ragione del fatto che i trattamenti di dati personali – da censire nel Registro delle Attività di Trattamento – possono essere oggetto di violazioni (c.d. *data-breach*), è stata creata nella medesima piattaforma R.A.T. un'apposita Sezione dedicata alla tenuta del Registro delle Violazioni.

Nel richiamare la definizione di violazione dei dati personali, ovvero la "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*" di cui all'art. 4, punto 12 del GDPR, si rammenta che i Dirigenti delle Strutture regionali, in qualità di Designati al trattamento, sono tenuti anche alla gestione di tali violazioni. Ciò implica, da parte dei medesimi Dirigenti designati, la documentazione di tutte le violazioni di dati personali, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché delle relative circostanze e conseguenze e dei provvedimenti adottati (art. 33, par. 5, GDPR), all'interno di apposito Registro delle Violazioni, oltre che l'obbligo di fornire tale documentazione, su richiesta, al Garante Privacy in caso di accertamenti.

Pertanto, con il presente documento si forniranno indicazioni operative anche per la corretta gestione del Registro delle Violazioni, integrato nella piattaforma che ospita il Registro delle Attività di trattamento, da parte dei Dirigenti designati.

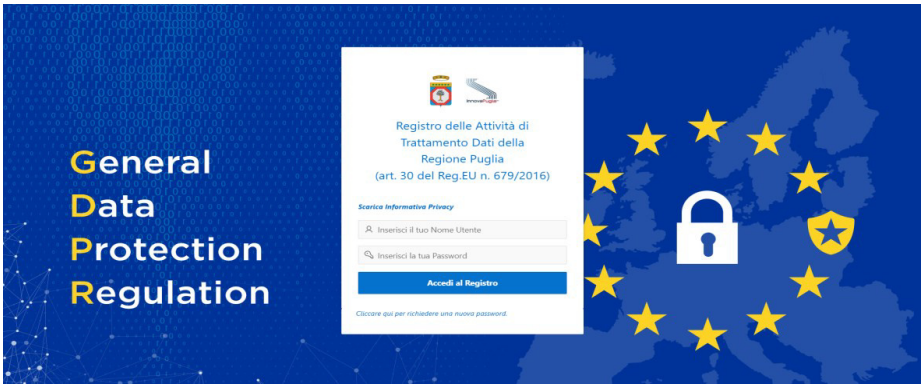
2. Accesso all'applicazione

Per poter avviare la gestione del Registro delle Attività di Trattamento di dati personali della Regione Puglia sulla relativa Piattaforma digitale è necessario dotarsi di credenziali di accesso.

A tal fine sulla *Home Page* della intranet NoiPA – Puglia, in basso a destra, è stata predisposta una *box* denominata "Credenziali Registro dei trattamenti GDPR", per mezzo della quale è possibile trasmettere al Centro Servizi le richieste per il rilascio delle suddette credenziali.

Una volta acquisite le credenziali, si può accedere al Registro secondo la procedura di seguito illustrata con il supporto delle singole schermate.

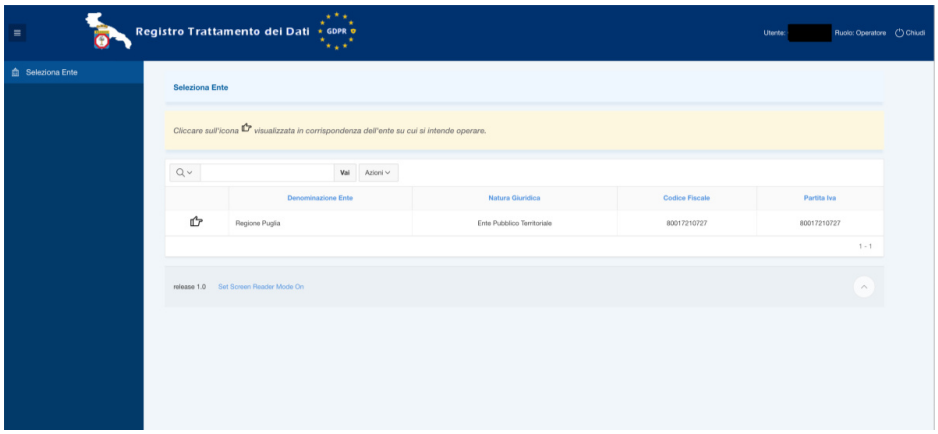
Si riporta di seguito la prima videata alla procedura, dove viene richiesto l'inserimento di Nome Utente e Password, cliccando poi sul pulsante Accedi al Registro.
Al primo accesso alla procedura, il sistema richiede all'operatore di impostare una nuova password. La nuova password sostituisce quella rilasciata dal Centro Servizi e dovrà essere utilizzata per gli accessi successivi. Nel caso in cui l'operatore dovesse averla dimenticata, potrà richiedere una nuova password, cliccando sul collegamento ***Cliccare qui per richiedere una nuova password***.



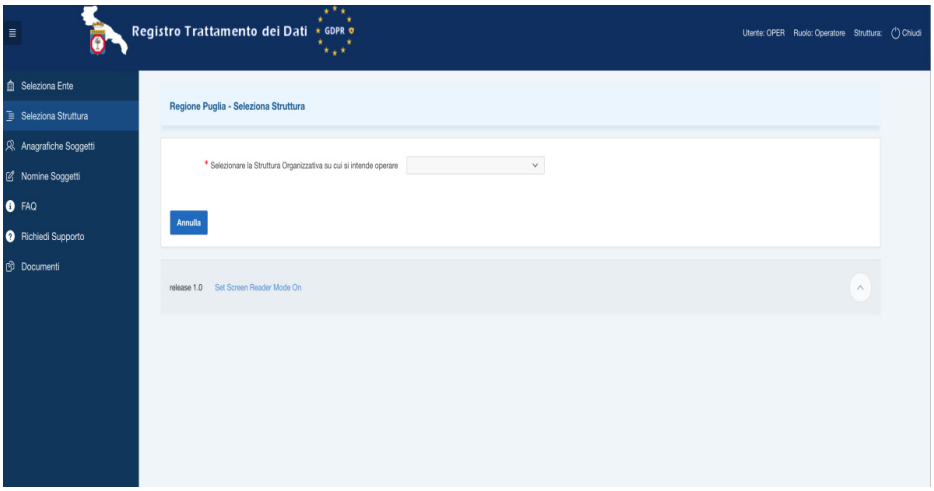
Nella suddetta *box* "Credenziali Registro dei trattamenti GDPR" è inoltre presente il collegamento denominato "***Scarica Informativa Privacy***", dal quale sarà possibile scaricare, cliccando sul relativo pulsante, l'Informativa privacy generale afferente il Registro delle Attività di Trattamento Dati della Regione Puglia (art. 30 del Reg.EU n. 679/2016).

3. Ente e Struttura nella quale si opera

Come prima operazione, è necessario selezionare l'Ente su cui si opera, cliccando sull'icona corrispondente, che nel caso specifico è generalmente "Regione Puglia", come nella schermata in basso.



Per quanto riguarda la struttura organizzativa in cui si opera, la schermata successiva viene visualizzata invece solo nel caso in cui l'operatore sia abilitato ad operare su più strutture organizzative: in tal caso il sistema richiederà di specificare la struttura su cui si intende operare.
Dunque, l'operatore abilitato ad operare su più strutture, visualizzerà un menù a tendina per la selezione della struttura sulla quale operare. L'asterisco in rosso indica l'obbligatorietà di compilazione del campo.

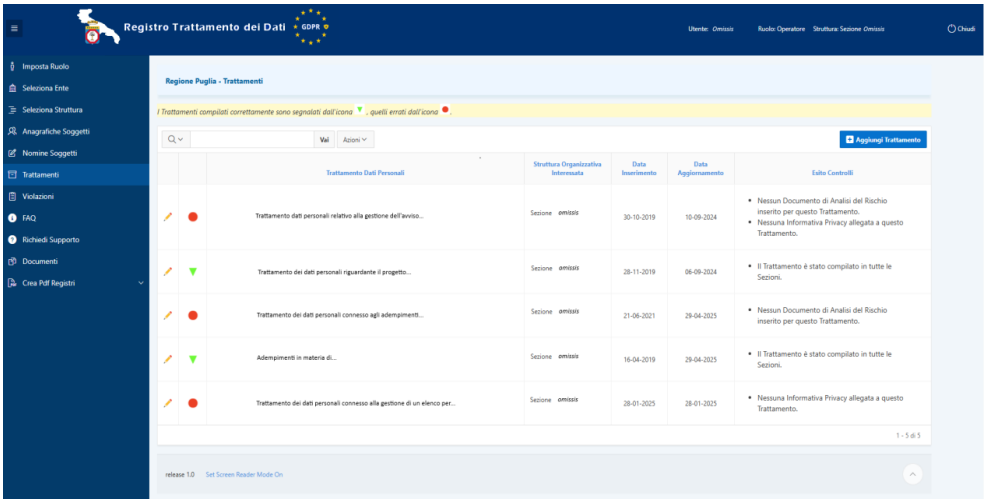


Una volta selezionata la struttura organizzativa su cui operare, il sistema presenta l'elenco dei trattamenti già censiti, come specificato nel successivo paragrafo 4.
Per gli operatori abilitati ad operare su più strutture sarà sempre possibile, attraverso la funzione di menu **Seleziona Struttura,** cambiare la struttura su cui operare senza uscire dalla procedura.

4. Elenco trattamenti

La schermata riportata di seguito consente di visualizzare l'elenco dei trattamenti già censiti e registrati per la struttura su cui si sta operando.
Per modificare un trattamento presente in elenco è necessario cliccare sull'icona raffigurante una matita in corrispondenza del trattamento di interesse. Per salvare le modifiche nel *database* è necessario cliccare sul pulsante **Aggiorna**.
Per inserire un nuovo trattamento, è necessario cliccare sul pulsante **Aggiungi Trattamento**.

Nella schermata "Trattamenti", di seguito rappresentata a stralcio, viene riportata la colonna finale "Esito controlli", tramite la quale è possibile verificare la corretta e completa compilazione di tutte le sezioni del Registro.



5. Trattamento dati effettuato da Regione Puglia in qualità di Titolare del trattamento

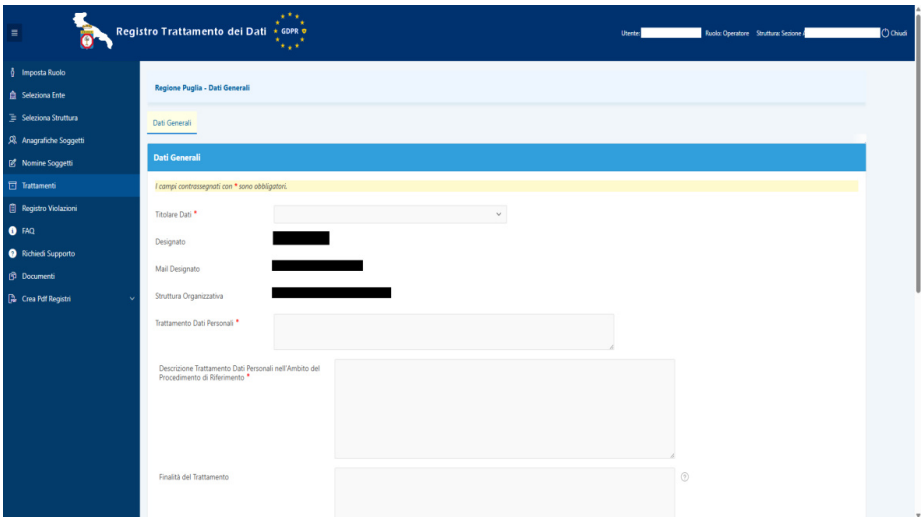
Per ogni nuovo trattamento effettuato dalla Regione in qualità di Titolare del trattamento, il sistema richiede la compilazione delle seguenti schermate:

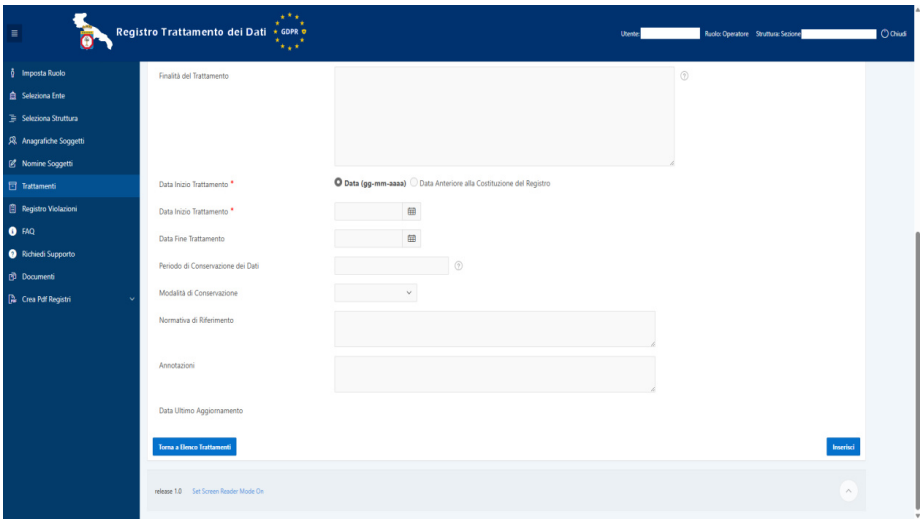
- Dati generali
- Contitolari
- Responsabili Esterni
- Persone Autorizzate
- Categorie dati trattati e base giuridica
- Categorie Trattamenti
- Soggetti Interessati
- Categorie Destinatari
- Trasferimenti
- Misure di Sicurezza
- Asset
- Archivi
- Criteri per analisi dei rischi ed Eventuale DPIA
- Informativa Privacy
- Allegati ulteriori

5.1. Dati generali

I Dati generali costituiscono l'insieme di informazioni che identificano il trattamento, come raffigurato nella schermata in basso.

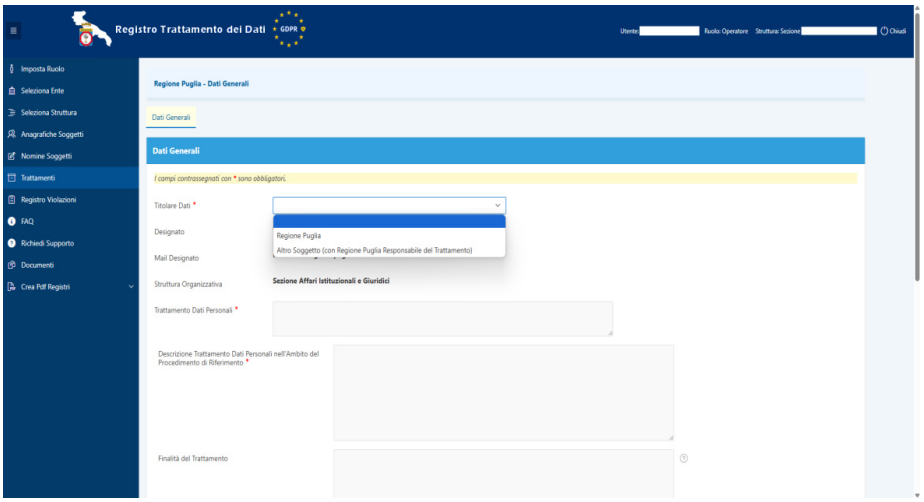
In fase di inserimento di un nuovo trattamento, la procedura valorizzerà automaticamente – in base al soggetto che procede all'inserimento ed alla Struttura organizzativa regionale di relativa appartenenza – i campi **Designato**, **Mail Designato** e **Struttura Organizzativa**, laddove il Designato è sempre il dirigente della Struttura organizzativa interessata ai sensi della D.G.R. 145/2019. Nel caso in cui la mail di contatto del Designato non fosse stato impostata in fase di registrazione della relativa nomina, la procedura imposterà il campo "Mail Designato" con il valore Non Specificata.





In fase di inserimento di un nuovo trattamento, cliccando sulla lista valori associata al campo **Titolare Dati**, è possibile selezionare uno dei seguenti valori:

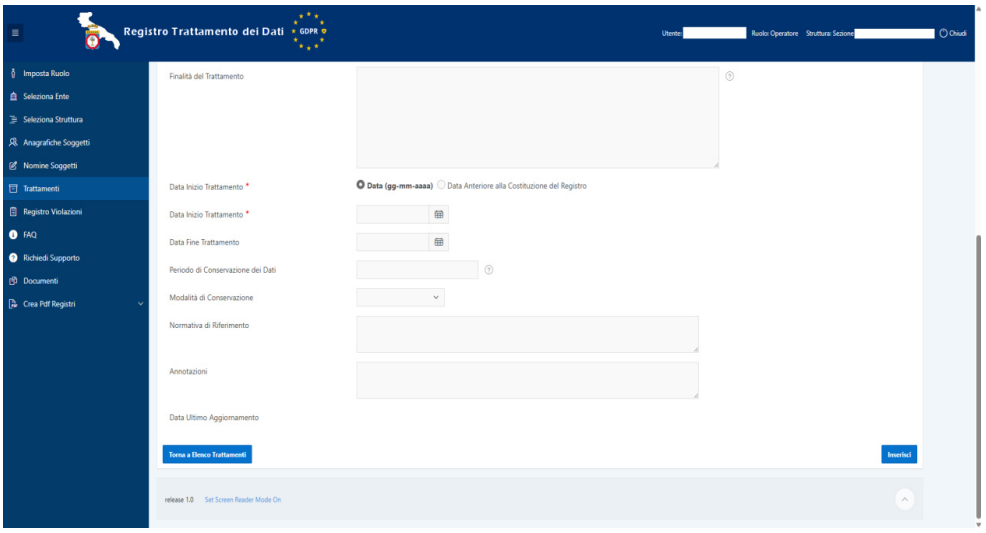
a. Regione Puglia
b. Altro Soggetto (con Regione Puglia Responsabile del Trattamento).



Selezionando come Titolare del trattamento dati la **Regione Puglia**, la procedura valorizzerà automaticamente i seguenti campi:

- Il nominativo del Responsabile Protezione Dati;
- La mail di contatto del Responsabile Protezione Dati.

A questo punto sarà necessario compilare tutti i campi relativi al trattamento dati, come di seguito schematizzato.



Nel campo **Trattamento Dati Personali** è necessario indicare quali operazioni di trattamento dati personali – riferiti esclusivamente a persone fisiche, e non anche a persone giuridiche – sono effettuate (ad es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di beneficiari di sussidi economico-sociali; trattamento dei dati sanitari degli utenti del S.S.R.; ecc.).

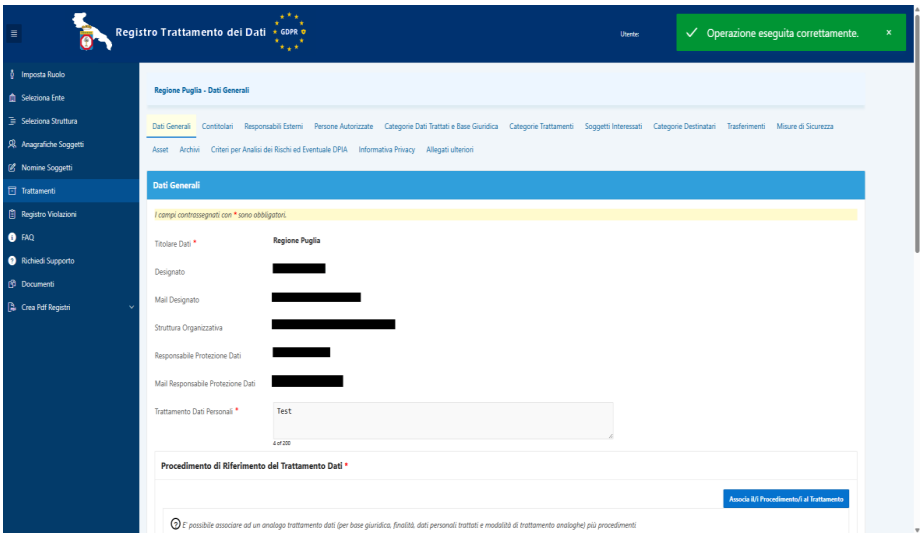
Nel campo **Descrizione Trattamento Dati Personali nell'Ambito dei Procedimenti di riferimento** è necessario inserire una breve descrizione dell'attività di trattamento dati personali svolta nell'ambito dei procedimenti amministrativi di riferimento, con indicazione delle sue principali caratteristiche.

Nel campo **Finalità del Trattamento** deve essere indicata la finalità del trattamento, con espressa indicazione della normativa di riferimento da cui discende tale finalità (ad es., "gestione, conservazione ed archiviazione documentale... ai sensi della L. n. x/xxxx").

Il campo **Data Inizio Trattamento** permette di impostare la data di avvio del trattamento. Se il trattamento è successivo alla data di costituzione del registro, occorre selezionare l'opzione **Data (gg-mm-aaaa)** e inserire la data nel formato richiesto; nel caso in cui il trattamento fosse antecedente alla data di costituzione del registro e non conosciuto/non determinato, occorre selezionare l'opzione **Data anteriore alla costituzione del registro**.

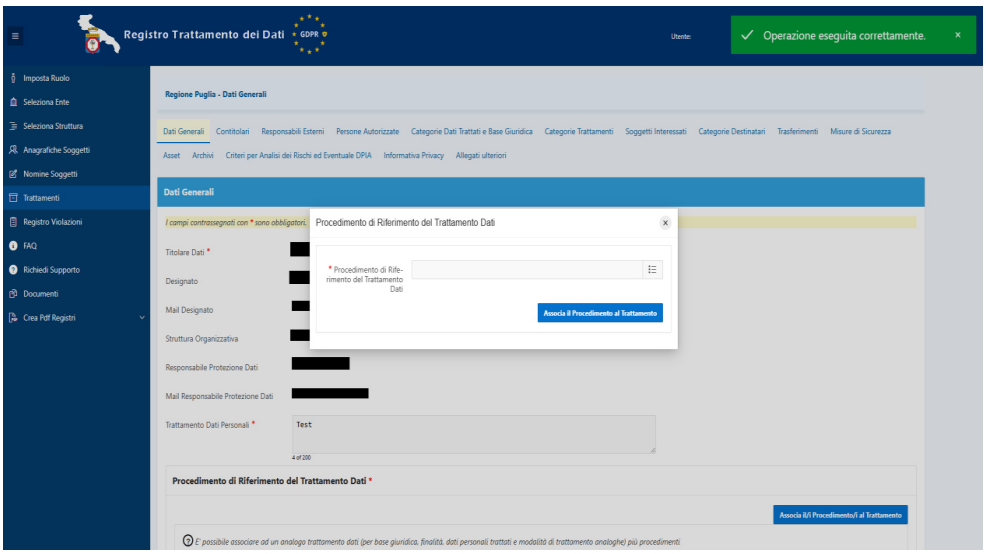
Nel campo **Periodo di Conservazione dei Dati** potranno essere indicati – ove possibile – i **"termini ultimi previsti per la cancellazione delle diverse categorie di dati",** che andranno definiti in base alla tipologia e finalità di trattamento (ad es. in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione ex art. 2220 del Codice civile). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri indicativi quali norme di legge o prassi settoriali (es. in caso di contenzioso, i dati saranno cancellati decorsi 12 mesi dal passaggio in giudicato della sentenza che ha definito il giudizio).
La durata di conservazione dei dati deve comunque coincidere con quella riportata nel "Manuale di conservazione e scarto dei documenti" dell'Ente Regione, ove disponibile.

Dopo aver compilato tutti i campi fin qui richiamati, per salvare i valori nel data-base occorre cliccare sul pulsante "Inserisci" e passare alla schermata successiva, che consentirà di inserire i dati generali relativi al trattamento dati personali di cui si opera il censimento nel RAT.

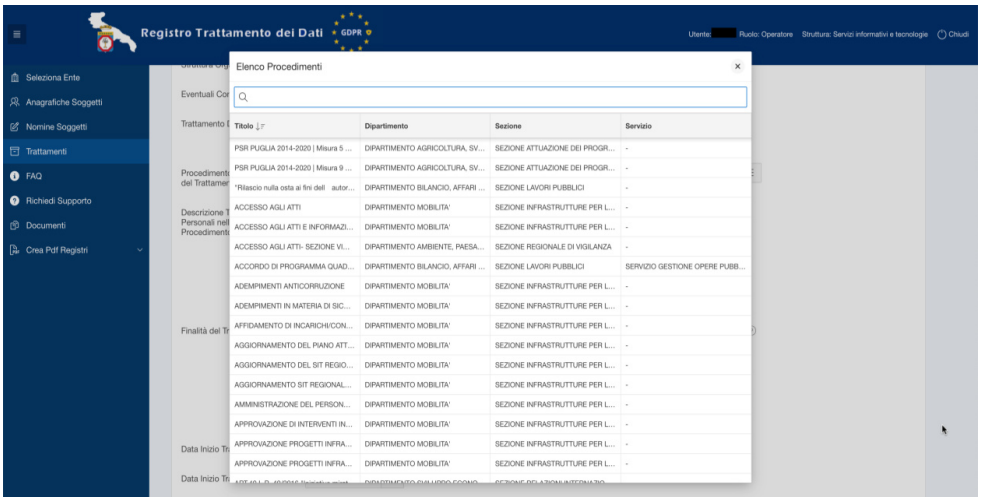


Al termine della compilazione della suddetta schermata, cliccando sul pulsante in basso a destra "Associa il/i Procedimento/i al Trattamento", si aprirà una seconda schermata dalla quale sarà possibile visualizzare l'elenco dei procedimenti amministrativi contenuti nel Catalogo dei Procedimenti pubblicato nella Sezione "Amministrazione Trasparente" del Portale della Regione

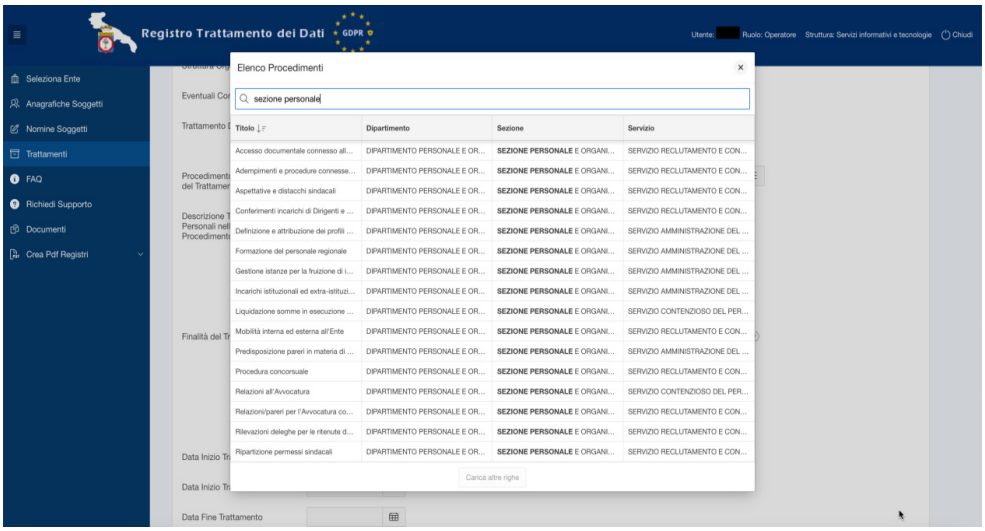
Puglia: da tale elenco andrà selezionato il procedimento amministrativo cui afferisce il trattamento di dati personali di riferimento nel RAT.



Ai fini della selezione del procedimento dl Catalogo Procedimenti, il sistema offre la possibilità di impostare un apposito filtro di selezione. Per procedere, occorre inserire la stringa di caratteri da ricercare nel campo di selezione individuato dall'icona raffigurante una lente di ingrandimento, e premere il pulsante Invio della tastiera. Tale stringa verrà ricercata in tutte le colonne contenute nella finestra (titolo, dipartimento, sezione, servizio).

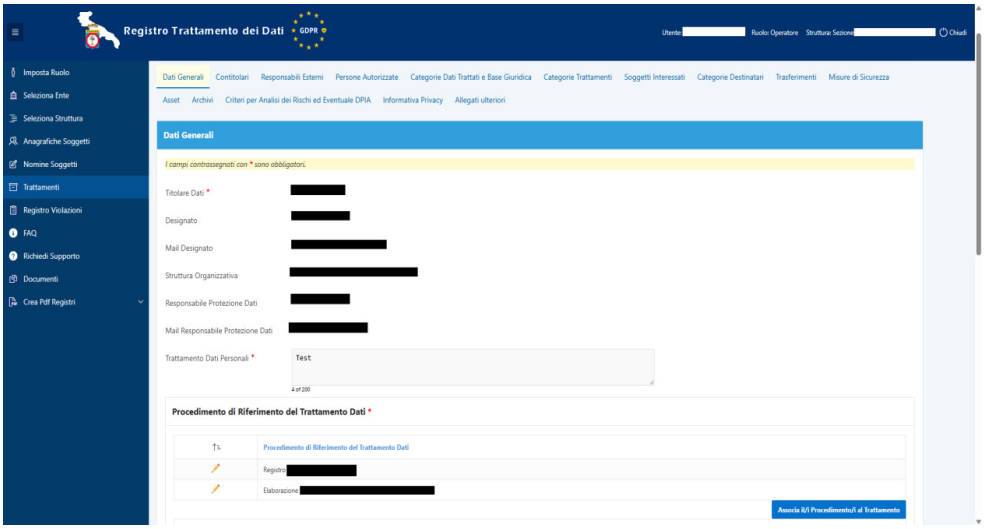


Ad esempio, volendo ricercare tutti i procedimenti della Sezione Personale, occorre inserire nel campo ***Sezione Personale*** (il carattere minuscolo o maiuscolo è indifferente) e cliccare sul tasto Invio: il sistema visualizza tutti i trattamenti che contengono all'interno dei campi visualizzati la stringa ***Sezione Personale***. Quindi, per selezionare il procedimento desiderato, bisogna semplicemente cliccare sulla riga corrispondente.



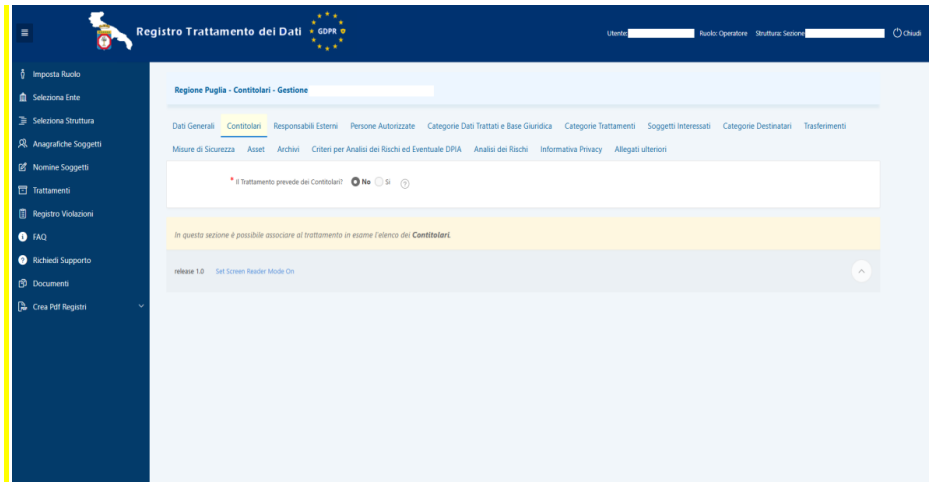
Preme precisare che il sistema permette di associare ad un trattamento di dati personali censito nel RAT uno o più procedimenti amministrativi presenti nel Censimento Procedimenti (caricandoli uno per volta), nell'ipotesi in cui il trattamento di dati personali in questione risulti connesso a più procedimenti ovvero tale trattamento presenti – con riferimento a più procedimenti – le medesime caratteristiche in termini di contesto, finalità, base giuridica e ruoli privacy degli attori coinvolti.

Nella schermata seguente, a titolo meramente esemplificativo, si riporta un esempio di due procedimenti associati ad un unico trattamento di dati personali.

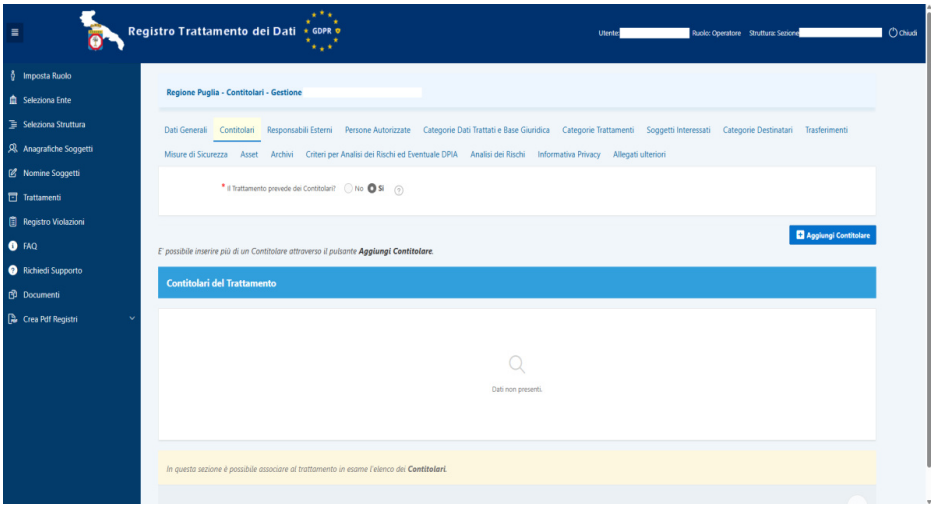


5.2. Contitolari

La scheda **Contitolari** permette all'operatore di indicare se il trattamento che si sta inserendo prevede o meno dei Contitolari del trattamento, cioè soggetti che condividano con la Regione (Titolare) la definizione di finalità e mezzi del trattamento di dati in questione.
Se si seleziona l'opzione **No,** il sistema non visualizzerà il pulsante "**Aggiungi Contitolare"**.



Viceversa, se si seleziona l'opzione **Si**, la procedura visualizzerà la scheda **Contitolari** per consentire l'inserimento delle informazioni relative ad uno o più contitolari del trattamento.



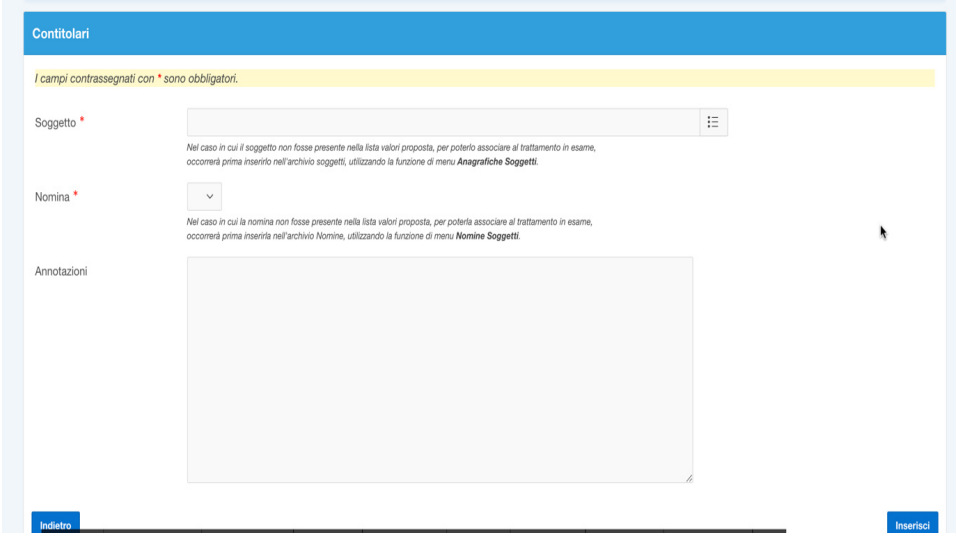
Si ricorda che la contitolarità del trattamento di dati personali è disciplinata nel Reg. UE 679/2016 (GDPR) all'art. 26, in base al quale:

- sono contitolari del trattamento due o più titolari che stabiliscono congiuntamente le finalità e i mezzi del trattamento;
- i contitolari del trattamento devono redigere un accordo interno (cd. accordo di contitolarità) che definisca le responsabilità di ciascun contitolare in termini di *privacy compliance* durante il trattamento, con particolare riferimento all'esercizio dei diritti dell'interessato, agli obblighi di rendere l'informativa ex artt. 13 e 14 GDPR ed ai ruoli e rapporti dei contitolari con gli interessati;
- l'accordo può designare un unico punto di contatto per gli interessati;
- il contenuto essenziale dell'accordo è messo a disposizione dell'interessato ex art. 26, n. 2, GDPR.

Il sistema offre la possibilità - cliccando sull'icona elenco localizzata in corrispondenza del campo “Soggetto” - di aprire una nuova finestra contenente l'elenco dei Contitolari già inseriti nel sistema. Nel caso in cui il soggetto non fosse inserito nella lista proposta, per poterlo associare al trattamento in questione occorrerà prima inserirlo nell’archivio “Soggetti”, utilizzando la funzione di menù **Anagrafiche Soggetti** presente in alto a sinistra della *Home page.*

Analogo procedimento vale per il campo “Nomina”: per poterlo associare al trattamento dati personali oggetto di compilazione, occorrerà prima inserirlo nell’archivio “Nomine” utilizzando la funzione di Menù **Nomine Soggetti** presente in alto a sinistra della *Home page.*

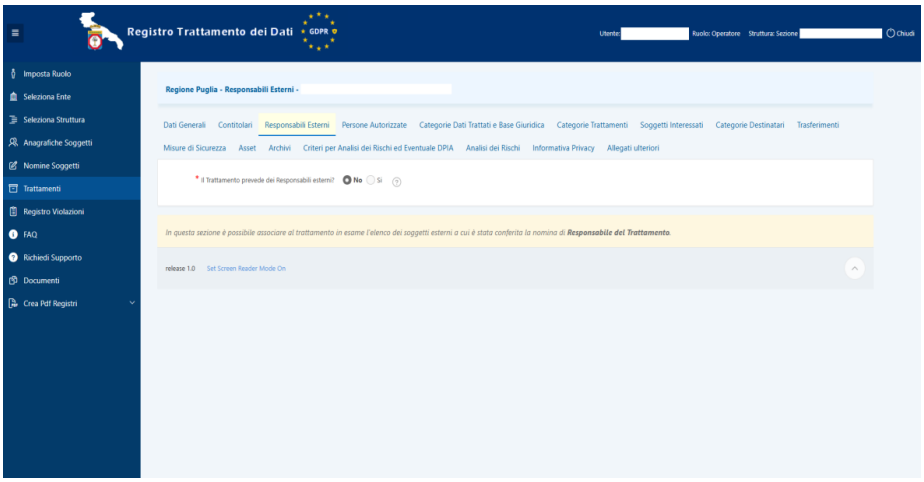
Per l’inserimento del Contitolare nell’archivio Soggetti e nell’archivio Nomine si seguano le indicazioni di dettaglio fornite al punto 5.3 per l’inserimento del Responsabile del trattamento, cui si rinvia.



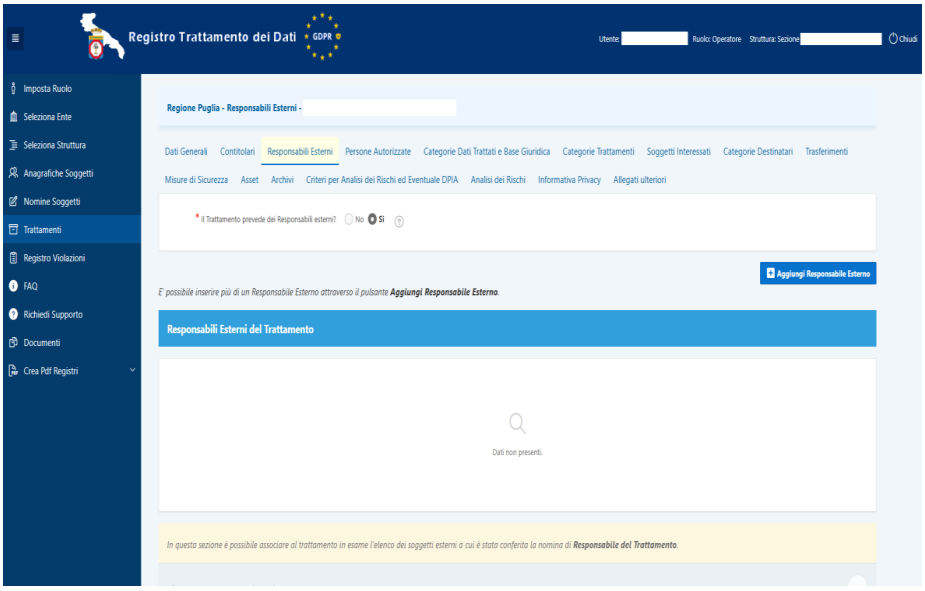
5.3. Responsabili Esterni

Il sistema consente di segnalare l’eventuale coinvolgimento nel trattamento in esame di soggetti esterni all’Amministrazione regionale, individuati quali Responsabili del trattamento *ex* art. 28 GDPR. Giova rammentare che il Responsabile del trattamento, ai sensi dell’art. 4, n. 8, del GDPR, è *“la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento”*. A titolo esemplificativo, sono responsabili *ex* art. 28 GDPR i fornitori di beni/servizi nei confronti dell’intera Amministrazione regionale o di singole Strutture organizzative dell’Ente (ad es. servizi informatici, consulenze legali, ecc.) che implicano, per lo svolgimento degli adempimenti contrattuali, il trattamento di dati personali in possesso dell’Ente.

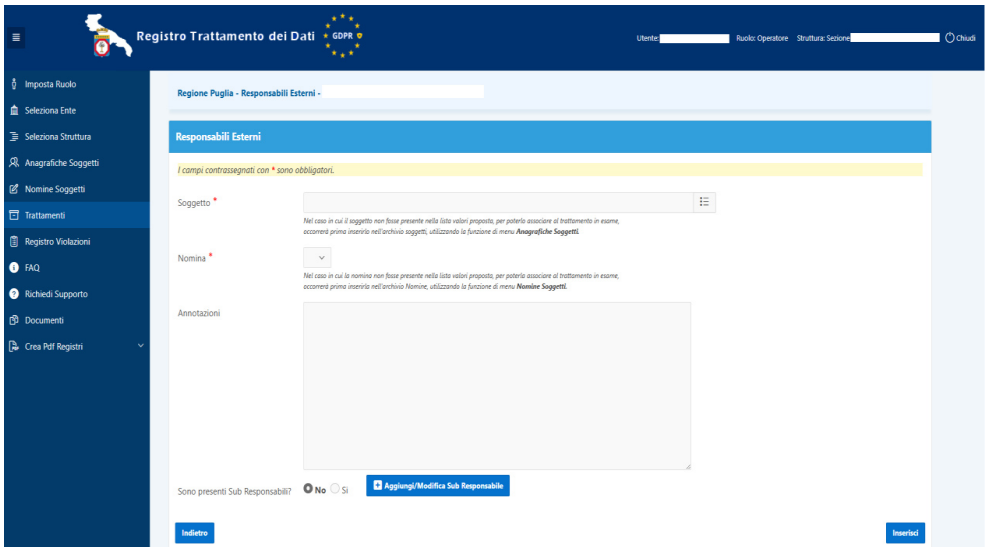
In questa Sezione, pertanto, viene prima di tutto richiesta l’eventuale presenza di Responsabili del trattamento (opzione SI/NO).



Se la risposta è positiva, ai fini dell'inserimento nel sistema di un Responsabile del trattamento, occorre cliccare sul pulsante "Aggiungi Responsabile Esterno" e passare alla schermata successiva.

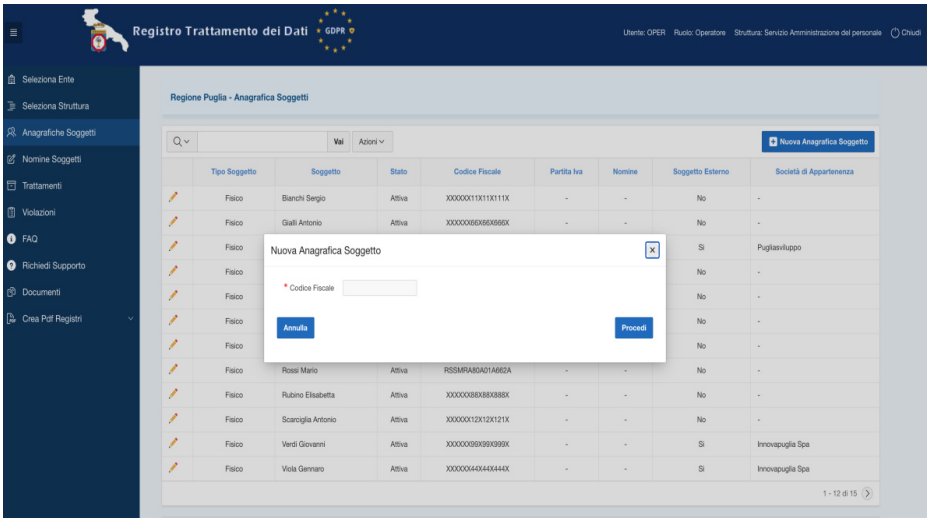


Il sistema offre la possibilità - cliccando sull'icona elenco localizzata in corrispondenza del campo "Soggetto" - di aprire una nuova finestra contenente l'elenco dei Responsabili già inseriti nel sistema.

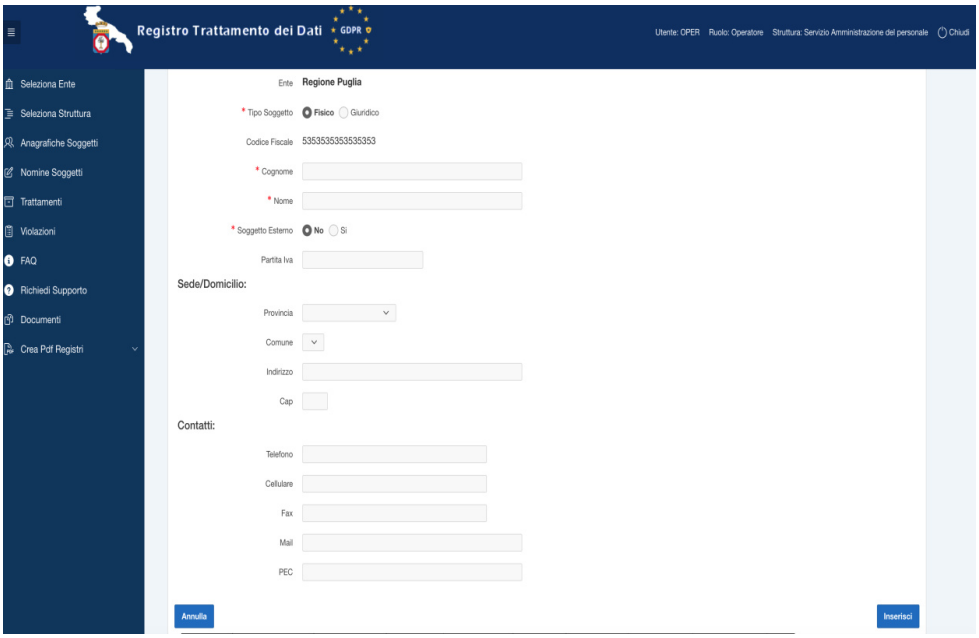


Nel caso in cui il "Soggetto" non fosse presente nella lista proposta, per poterlo associare al trattamento in esame occorre prima inserirlo nell'Archivio "Soggetti", utilizzando la funzione di menù **Anagrafiche Soggetti** presente in alto a sinistra della *Home page.*
Analogo procedimento vale per il campo "Nomina": per poterlo associare al trattamento di dati personali oggetto di compilazione, occorrerà prima inserirlo nell'archivio "Nomine" utilizzando la funzione di Menù **Nomine Soggetti** presente in alto a sinistra della *Home page*.

La schermata **Anagrafica Soggetti**, accessibile dopo aver cliccato il pulsante **Nuova Anagrafica Soggetto**, chiede di specificare il codice fiscale del soggetto che si intende registrare, in modo da non duplicare l'inserimento di un soggetto già presente in archivio.

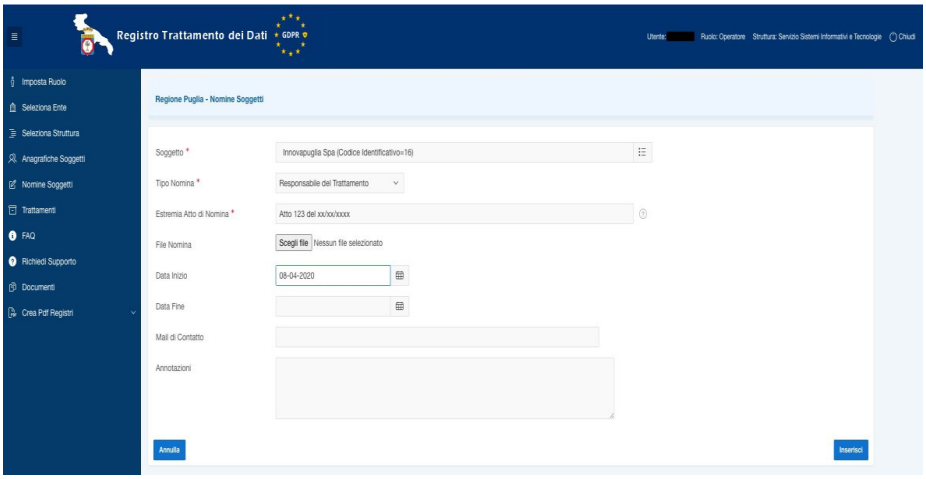


La schermata successiva chiede di specificare alcune informazioni sul Soggetto da inserire come Responsabile che, una volta inserite, andranno validate al fine del salvataggio cliccando il pulsante **Inserisci**.

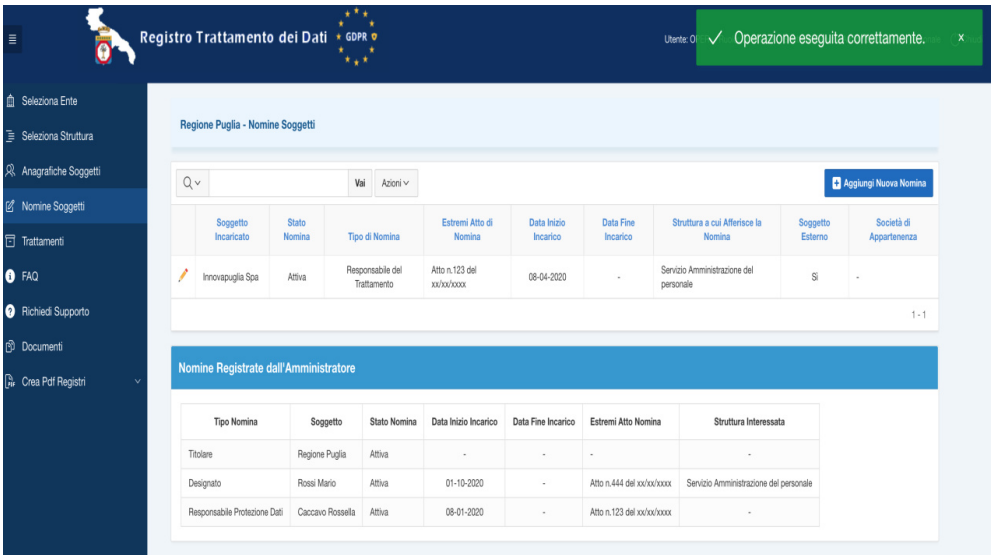


Una volta completata l'operazione preliminare di registrazione in Anagrafica Soggetti, si può procedere al caricamento delle informazioni relative alla nomina utilizzando la funzione di menù **Nomine Soggetti**. A tal fine sarà necessario compilare i campi obbligatori della schermata che segue.

Cliccando sull'icona elenco posta in corrispondenza del campo **Soggetto** si aprirà un menù a tendina contenente l'elenco dei Soggetti presenti in archivio, da cui selezionare il Soggetto a cui si riferisce la nomina.

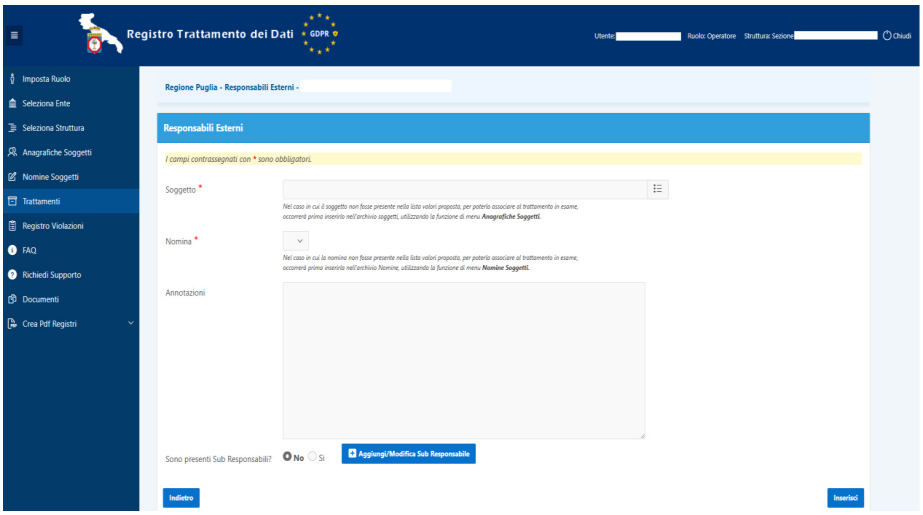


Una volta compilati tutti i campi richiesti, sarà necessario cliccare sul pulsante **Inserisci** per salvare i valori impostati nel data base.

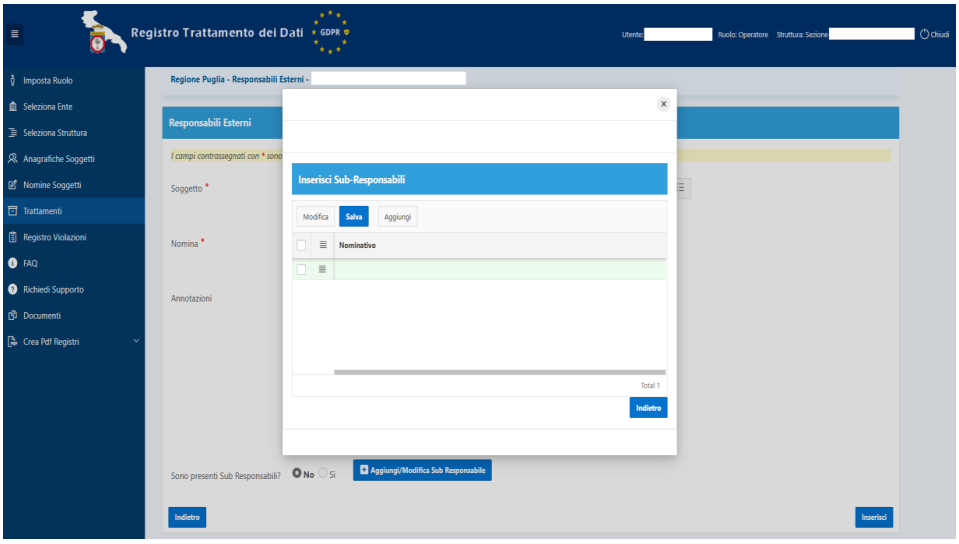


La Sezione relativa ai Responsabili esterni prevede anche uno specifico campo dedicato alla presenza di eventuali sub-Responsabili del trattamento, che possono essere designati da parte di un Responsabile (art. 28, par. 4 GDPR) per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "*non gli è in alcun modo imputabile*" (art. 82, par. 1 e par. 3 GDPR). Pertanto, il Responsabile del Trattamento nominato dal Titolare può delegare alcune specifiche attività a Sub-responsabili, ma solo se autorizzato dal Titolare.
Si rinvia, a tale proposito, alla disciplina regionale con la quale sono stati approvati i modelli di Accordi *Data Protection*: Accordo Titolare/Responsabile ex art. 28 GDPR e accordo di contitolarità ex art. 26 GDPR. In particolare, nel modello di accordo di nomina del Responsabile del trattamento da parte del Titolare viene disciplinata, tra le altre cose, la modalità di nomina del Sub-Responsabile del trattamento da parte del Responsabile, prevedendo altresì che il Responsabile del trattamento deve sottoporre a preventiva autorizzazione scritta e specifica del Titolare, nella persona del dirigente Designato, qualsiasi affidamento di trattamento ad eventuale sub-responsabile.

Ciò premesso, ai fini dell'inserimento di un sub-responsabile esterno nella sezione del RAT qui illustrata, occorre previamente selezionare l'opzione "**Si"** alla domanda "Sono presenti Sub-Responsabili?" e, successivamente, cliccare sul pulsante "Aggiungi/Modifica Sub Responsabile" passando alla schermata successiva.



Nella schermata che a questo punto si genera sarà possibile aggiungere i nominativi dei Sub-Responsabili coinvolti.

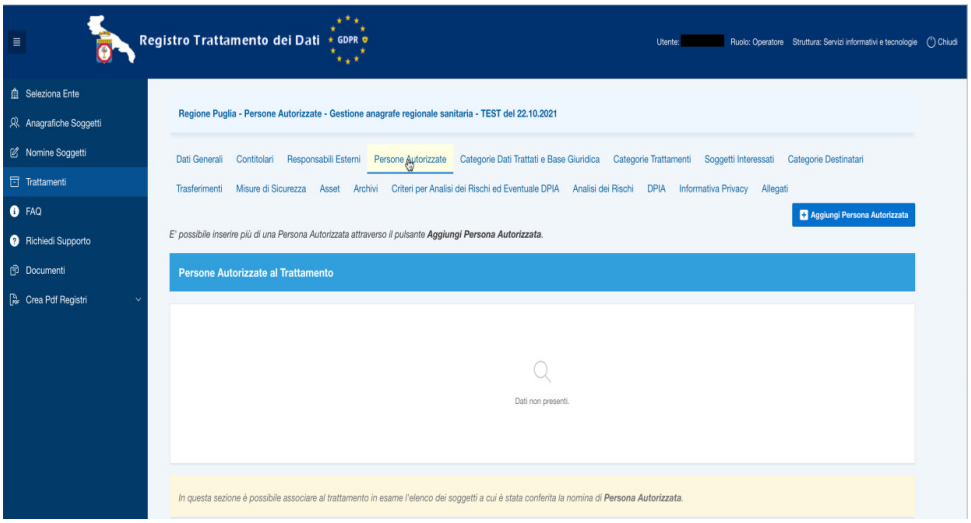


5.4 Persone Autorizzate

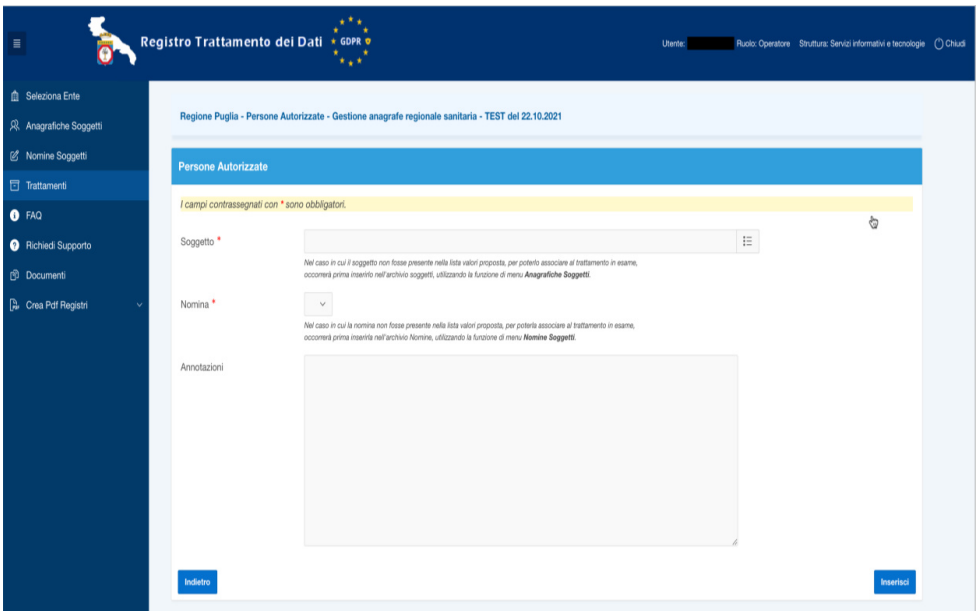
Tra i soggetti coinvolti nel trattamento di dati personali il GDPR include, all'art. 4, n. 10, ed all'art. 29, le c.d. *"persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".* Si tratta dei cd. Autorizzati al trattamento, che il sistema consente di indicare con riferimento a ciascun trattamento di dati personali inserito nel Registro.

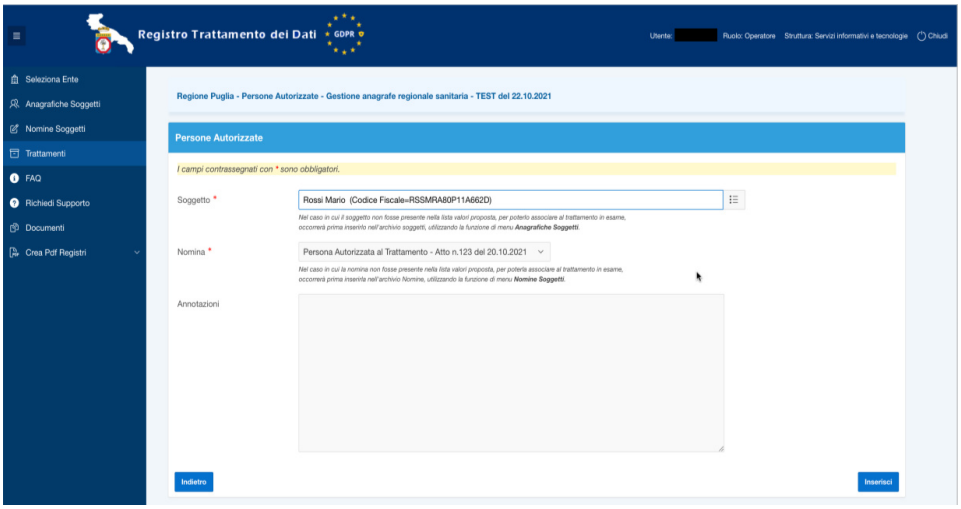
Nell'ambito della Regione Puglia, i Dirigenti – in qualità di Designati al trattamento dei dati per le strutture regionali della Giunta regionale *ex* DGR n. 145 del 30/1/2019, All. A, punto 3.2, lett. d) ed e) – provvedono per conto del Titolare del trattamento *"alla nomina delle persone autorizzate al trattamento con proprio atto di organizzazione, individuando le operazioni di trattamento dei dati personali strettamente indispensabili per lo svolgimento delle attività loro assegnate e segnatamente impartiscono istruzioni alla persona autorizzata, in modo da assicurare il pieno rispetto dei principi richiamati ed in particolare della sicurezza del trattamento"*.

Nelle schermate che seguono, relative alla sezione “Persone autorizzate” del RAT, è indicata la procedura per segnalare il coinvolgimento, nel trattamento dati personali in esame, di **soggetti Autorizzati.**



Secondo la medesima procedura già descritta in dettaglio al precedente punto 5.3 della presente Guida con riferimento al “Responsabile del trattamento”, dopo aver cliccato sul pulsante **Aggiungi Persona Autorizzata,** nel caso in cui il “Soggetto” non fosse presente nella lista proposta, per poterlo associare al trattamento in esame occorre prima inserirlo nell’archivio “Soggetti”, utilizzando la funzione di menù **Anagrafiche Soggetti**.
Analogo procedimento vale per il campo “Nomina”: per poterlo associare al trattamento di dati personali oggetto di compilazione, occorrerà prima inserirlo nell’archivio “Nomine” utilizzando la funzione di Menù **Nomine Soggetti.**



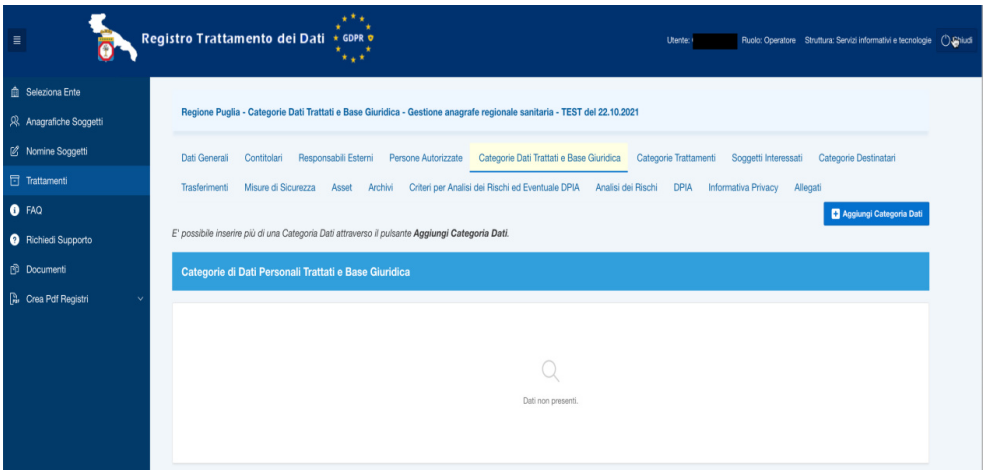


Dopo aver inserito i dati richiesti, occorre cliccare sul pulsante **Inserisci** per salvare i valori nel *data base.*

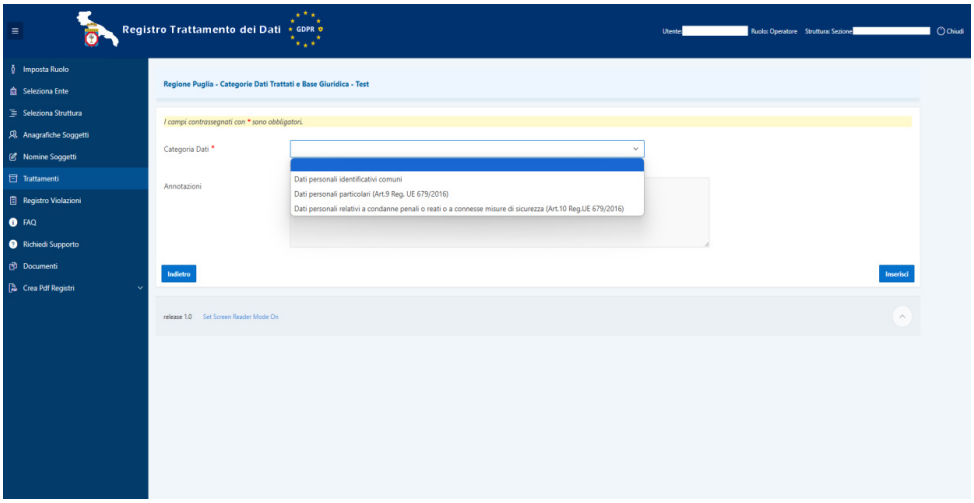
5.5 Categorie dati trattati e base giuridica

Il sistema consente di indicare la condizione che – ai sensi dell'art. 6, par. 1, ovvero dell'art. 9, par. 2, e dell'art. 10 del Regolamento UE 679/2016 – rende lecito il trattamento di dati (cd. base giuridica).
L'art. 6 del GDPR prevede infatti in linea generale che debba essere sempre indicata la base giuridica sulla scorta della quale vengono effettuate le operazioni di trattamento dati, la quale deve essere prevista dal diritto dell'Unione Europea o dal diritto dello Stato membro cui è soggetto il titolare del trattamento. Ove il trattamento riguardi categorie particolari di dati, ovvero gli *ex* dati sensibili (*"dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"*), sarà necessario indicare il riferimento alle condizioni di cui all'art. 9, par. 2, del GDPR; inoltre, in caso di trattamento di dati relativi a condanne penali o reati e a connesse misure di sicurezza, dovrà essere indicato il riferimento alle condizioni di cui all'art. 10 del GDPR.
Di regola la base giuridica per il trattamento dei dati da parte delle Pubbliche Amministrazioni è rinvenibile nell'obbligo legale al quale è soggetto il titolare del trattamento oppure nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, giusta previsione dell'art. 6, comma 1 del GDPR, rispettivamente, alla lett. c) per l'obbligo legale e alla lett. e) per l'esecuzione di un compito di interesse pubblico.

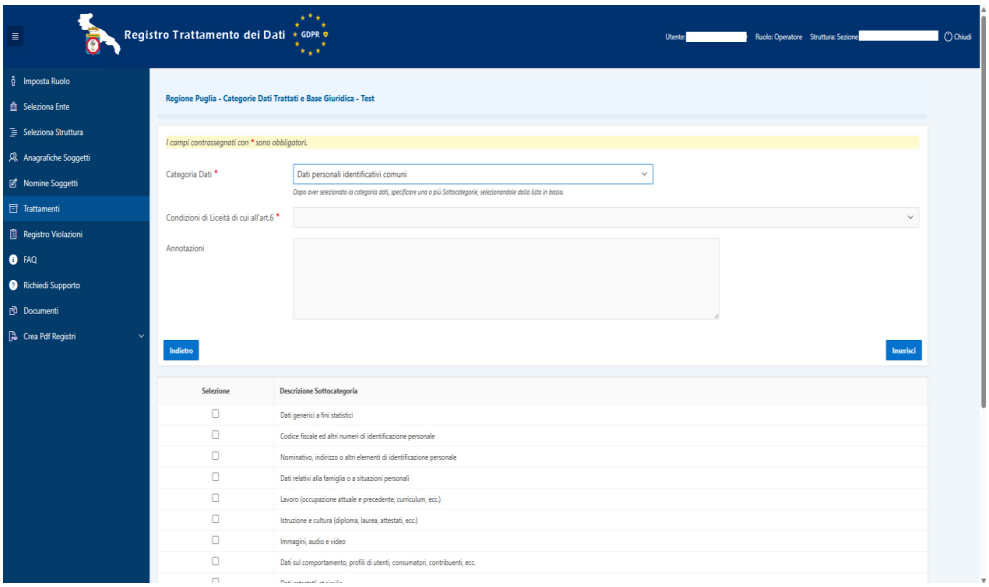
Ciò premesso, per inserire la categoria di dati trattati - come indicato nella schermata che segue - è necessario cliccare sul pulsante **Aggiungi Categoria Dati**.



Il primo campo della schermata da compilare è quello relativo alla **Categoria Dati** cui afferisce il trattamento di dati personali da inserire nel RAT, da scegliere - dal menù a tendina disponibile a sistema - fra le categorie riportate.

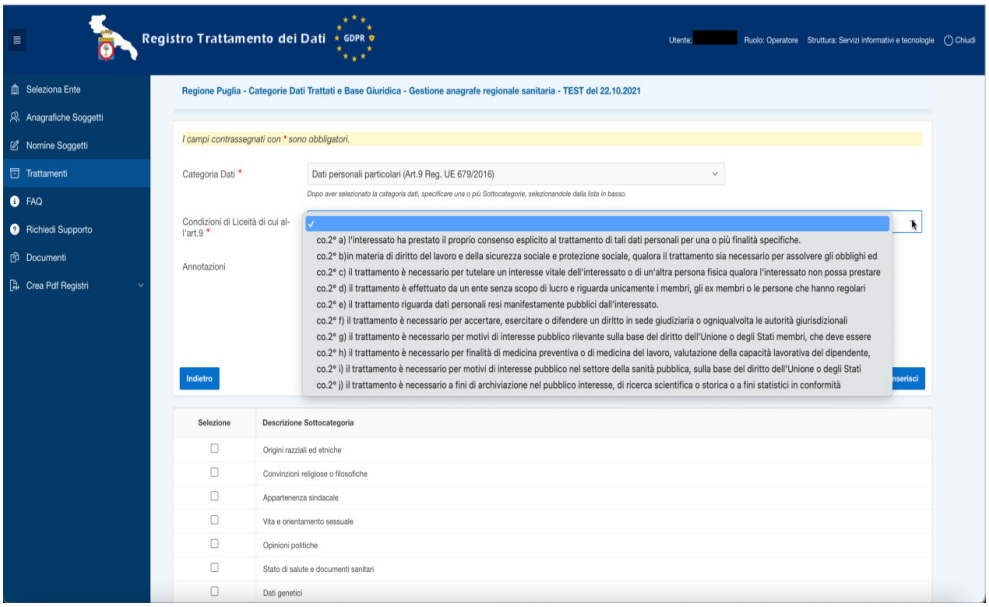


A seguito della selezione di una categoria dati, ad es. la categoria “Dati personali identificativi comuni”, la schermata si aggiorna di *default* (aggiornando il menù a tendina del pulsante “Condizioni di liceità”) con il solo elenco di basi giuridiche del trattamento che possono teoricamente riguardare i dati comuni in base alle previsioni del GDPR. A questo punto sarà necessario selezionare una dal menù a tendina, scegliendo quella che riferisce specificamente al trattamento in questione.
Si sottolinea che il sistema permette l’inserimento anche di più basi giuridiche tra quelle individuate dal GDPR e che sarà necessario, a tale fine, selezionare sempre preventivamente la categoria di dati interessati.



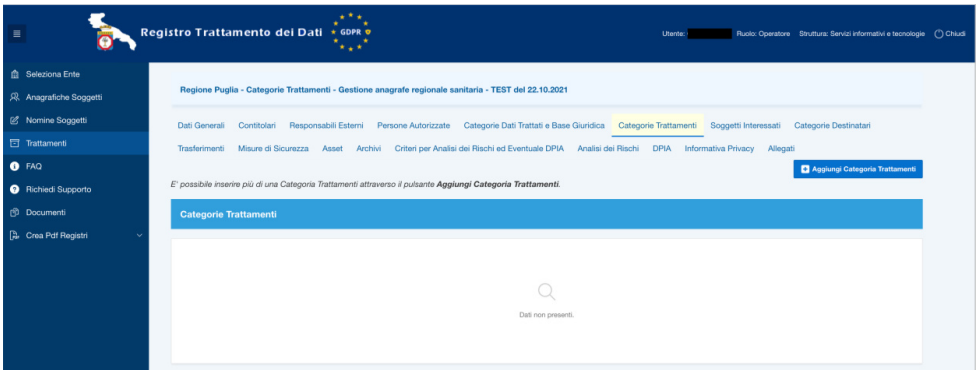
Una volta selezionata la categoria e sottocategoria di dati, nonché la base giuridica che giustifica il relativo trattamento, cliccando sul pulsante **Inserisci** viene salvato e visualizzato l'inserimento effettuato.

Gli stessi *step* fin qui descritti sono applicabili ai fini dell'inserimento delle altre categorie di dati, quali i "dati personali particolari" *ex* art. 9 GDPR e i "dati personali relativi a condanne penali o reati o a connesse misure di sicurezza" *ex* art. 10 GDPR.
Per entrambe le suddette categorie di dati, una volta effettuato l'inserimento, la schermata si aggiorna di *default* con le sole basi giuridiche che possono riguardare la categoria di dati prescelta. Anche in questo caso, cliccando sul pulsante **Inserisci** viene salvato e visualizzato l'inserimento effettuato.

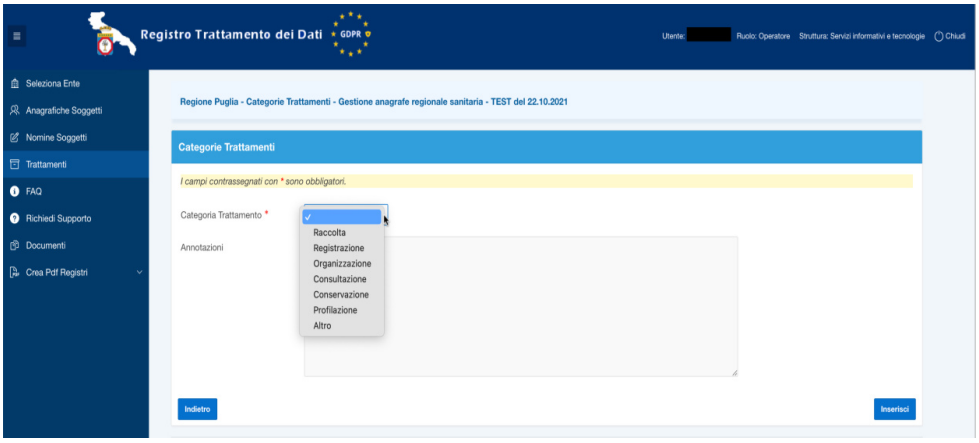


5.6 Categorie Trattamenti

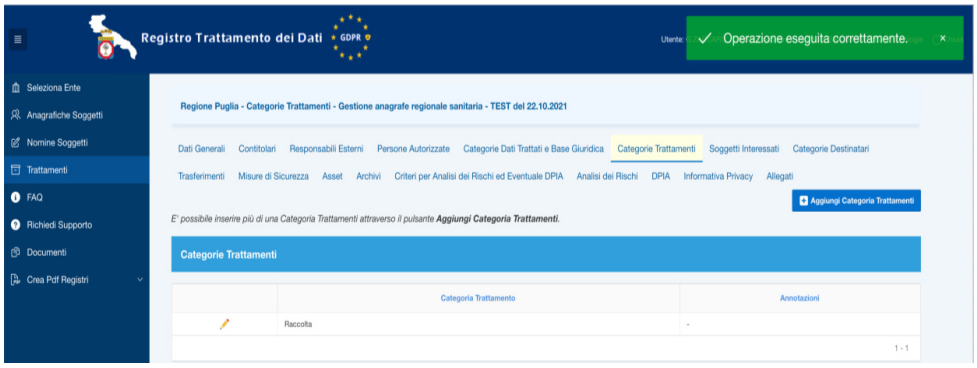
Per **"trattamento di dati personali"** si intende - secondo l'art. 4 del GDPR - *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, che consista in una delle attività di seguito indicate che abbia a oggetto dati personali o insiemi di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".* Lo svolgimento di tutte le suddette operazioni deve quindi essere tracciato nel Registro delle Attività di Trattamento.
Per inserire le varie categorie/operazioni di cui consta uno specifico trattamento, occorre cliccare sul pulsante **Aggiungi Categoria Trattamento**.



E' possibile selezionare, dal menù a tendina, una sola delle opzioni disponibili (raccolta, registrazione, organizzazione, ecc.) per il campo **Categoria trattamento** per volta. Il procedimento potrà essere ripetuto in presenza di più categorie/operazioni di trattamento.



Dopo aver selezionato la categoria di interesse, per salvare il valore nel database, occorre cliccare sul pulsante **Inserisci.** Come visualizzato nella schermata successiva, il sistema segnala la corretta esecuzione dell'operazione tramite il messaggio **Operazione eseguita correttamente**.

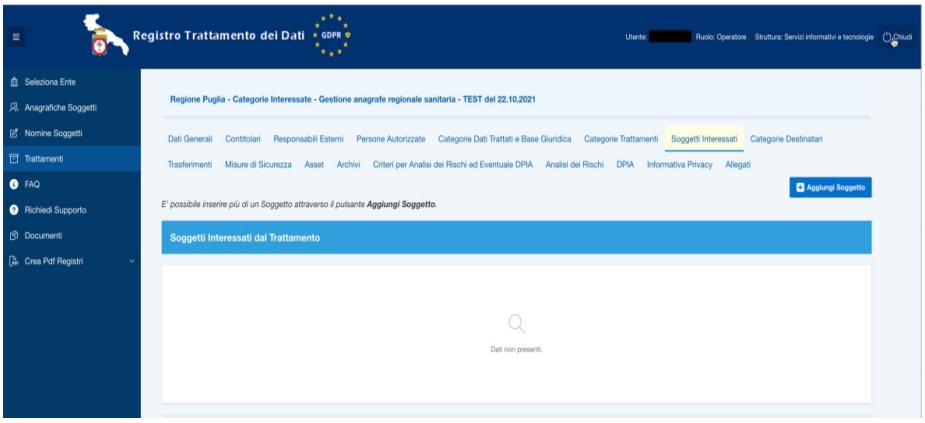


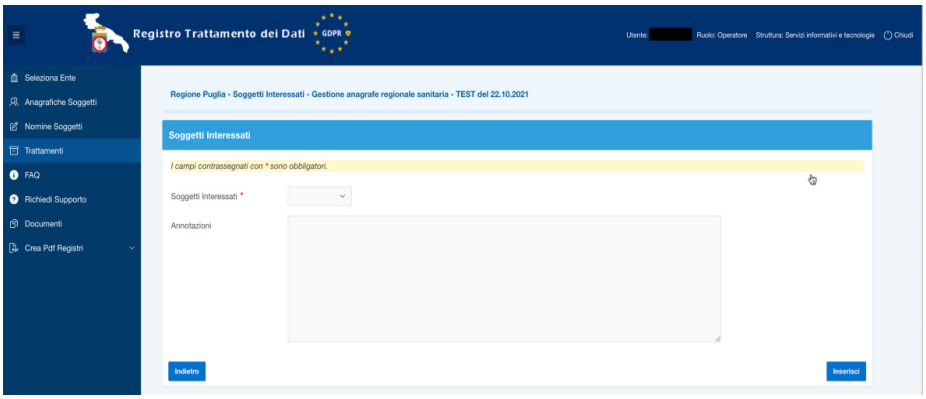
Se il trattamento dati prevede più categorie/operazioni fra quelle presenti nel menù a tendina, si procederà allo stesso modo per le altre categorie di trattamento.

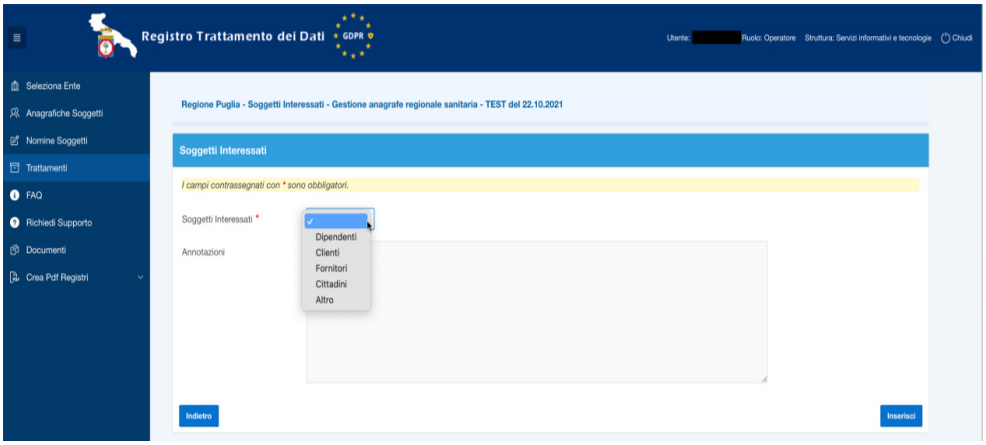
5.7 Soggetti interessati

Nel campo **Soggetti interessati** è necessario indicare una o più categorie di interessati al trattamento di dati personali, cioè le categorie di soggetti a cui si riferiscono i dati oggetto del trattamento.

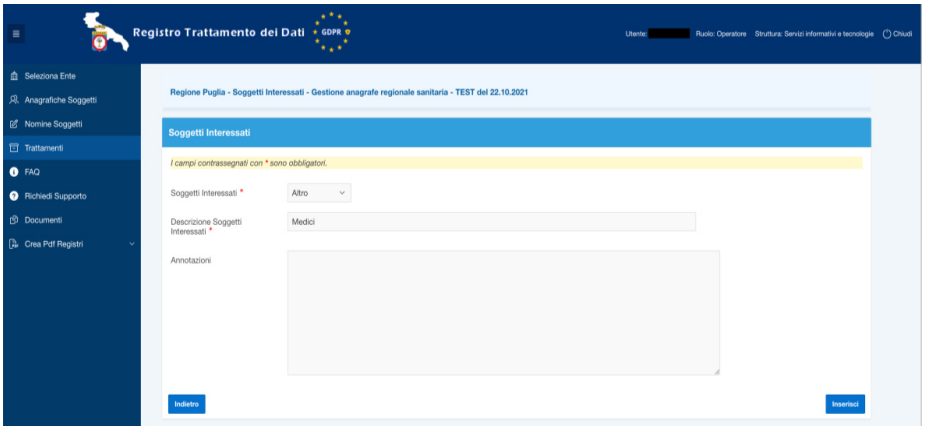
Per inserire un nuovo soggetto occorre cliccare sul pulsante **Aggiungi Soggetto**.
Comparirà quindi il campo Soggetti interessati, che presenta un menù a tendina, come raffigurato nelle schermate riportate di seguito.







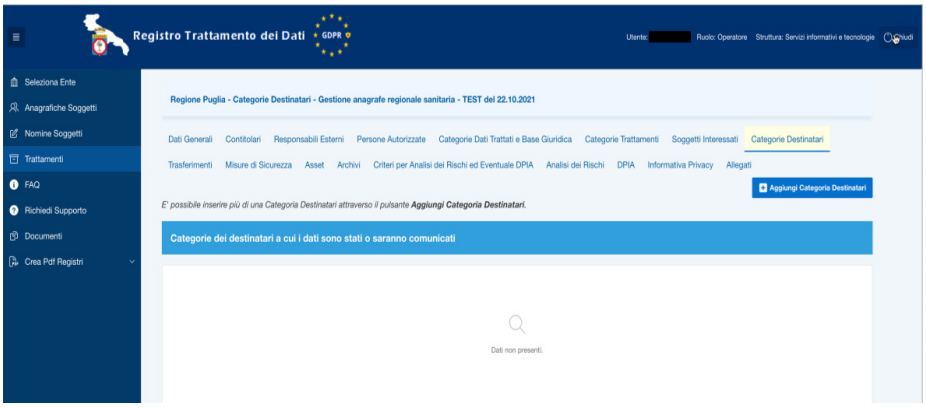
Anche in questo caso occorre selezionare una per volta, dal menù a tendina, le opzioni disponibili che si applicano al trattamento in questione.
Se la categoria di soggetti interessati dal trattamento per cui si effettua la compilazione non è tra quelle disponibili a sistema, sarà necessario selezionare l'opzione **Altro**: dopo aver selezionato tale opzione, il sistema visualizzerà il campo **Descrizione Soggetti Interessati** per consentire la specificazione della categoria di soggetti non presente nella lista di valori proposta. A questo punto, è necessario compilare il suddetto campo e infine cliccare sul pulsante **Inserisci**.



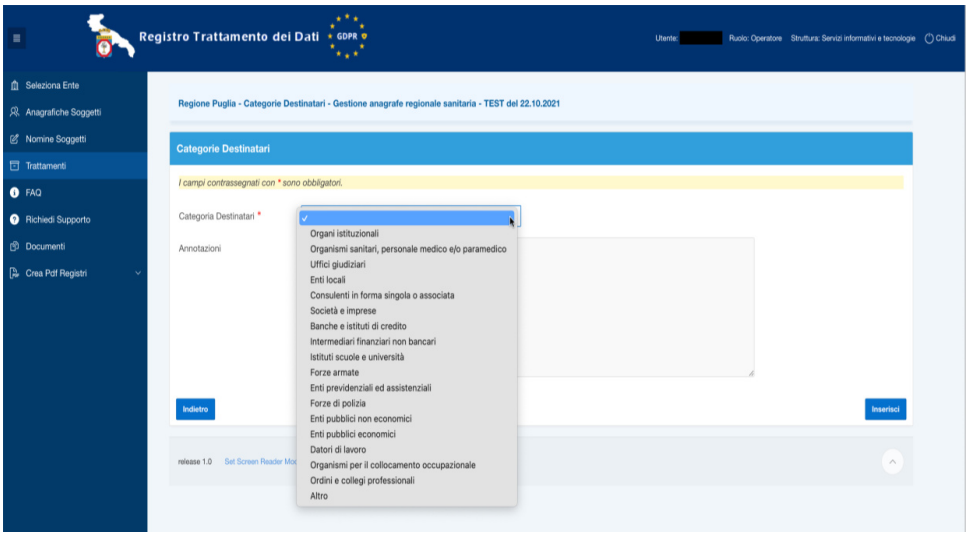
Il sistema segnalerà la corretta esecuzione dell'operazione richiesta tramite la visualizzazione del messaggio **Operazione eseguita correttamente**.

5.8 Categorie Destinatari

Nella schermata **"Categorie di destinatari"** devono essere riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere gli obblighi contributivi). Si ricorda che, ai sensi dell'art. 2-*ter*, comma 4, lett. a) D.lgs. n. 196/2003, come modificato dal D.Lgs. 101/2018, per "comunicazione" si intende *"il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione".*
Per inserire una categoria, occorre utilizzare il pulsante **Aggiungi Categoria Destinatari**.



Anche in questa schermata si chiede di selezionare le opzioni visualizzate, tra quelle presenti nel menù a tendina, una sola per volta.



Una volta selezionata l'opzione di interesse per il trattamento che si sta compilando, occorre cliccare sul pulsante **Inserisci** per salvare i dati nel database. Il sistema segnalerà la corretta esecuzione dell'operazione richiesta tramite la visualizzazione del messaggio **Operazione eseguita correttamente**.
Se la categoria dei destinatari non è tra quelle proposte dal sistema, è sempre possibile specificarne una aggiuntiva selezionando l'opzione **Altro** e poi inserendo la descrizione della categoria nel nuovo campo **Descrizione Categoria**.

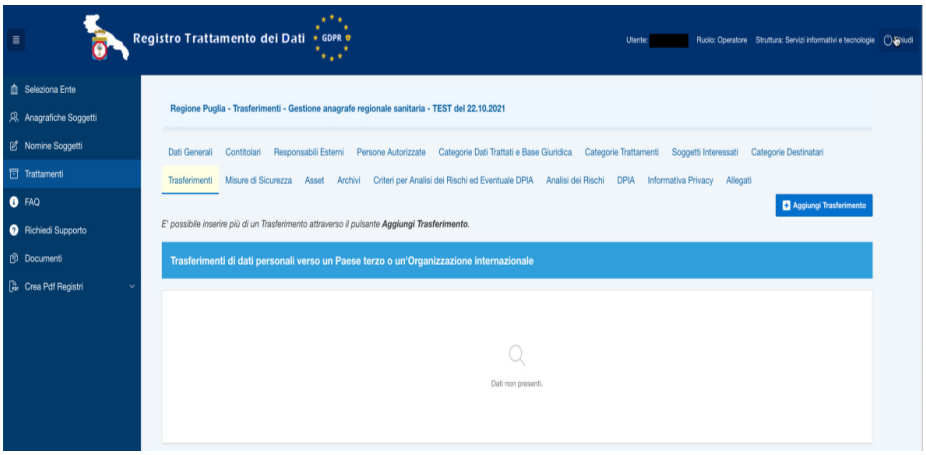
5.9 Trasferimenti

Nell'ipotesi in cui il trattamento implichi un trasferimento di dati personali verso Paesi terzi (al di fuori dell'UE) oppure verso organizzazioni internazionali, la schermata chiede di indicare la condizione che autorizza il trasferimento di dati personali.
Il Regolamento UE 679/2016 (GDPR), che all'art. 44 definisce il trasferimento come "*qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale*", consente infatti all'art. 45 i trasferimenti di dati personali verso Paesi terzi solo "*a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea*". In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento UE 2016/679).
Al riguardo, possono costituire garanzie adeguate:

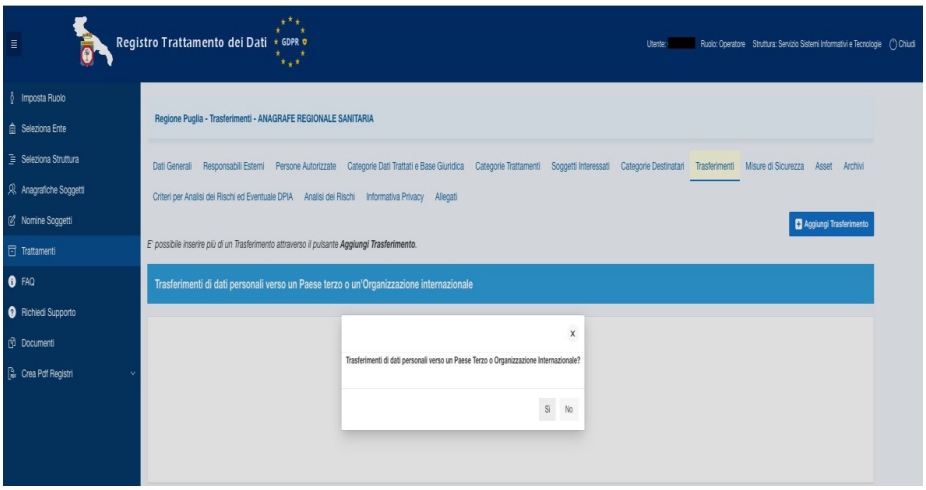
A. Senza autorizzazione da parte del Garante:
    1) gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
    2) le norme vincolanti d'impresa (art. 46, par. 2, lett. b);
    3) le clausole tipo (art. 46, par. 2, lett. c e lett. d);
    4) i codici di condotta (art. 46, par. 2, lett. e);
    5) i meccanismi di certificazione (art. 46, par. 2, lett. f).
B. Previa autorizzazione del Garante:
    1) le clausole contrattuali ad hoc (art. 46, par. 3, lett. a);
    2) gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b).
C. In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe che si verificano in specifiche situazioni (art. 49 del Regolamento UE 2016/679).

L'istituto dei "trasferimenti di dati personali" è applicabile, ad esempio, allorché vi sia la necessità di ricorrere all'adozione di servizi *cloud* forniti da Società che si trovano fuori dallo Spazio Economico Europeo (SEE). In tal caso, si è in presenza di tali trasferimenti sia quando i dati si trovano in server situati al di fuori del SEE, sia quando l'accesso viene effettuato da remoto da un paese terzo (ad esempio in situazioni di supporto) e l'archiviazione dei dati è effettuata in server situati all'interno del SEE.

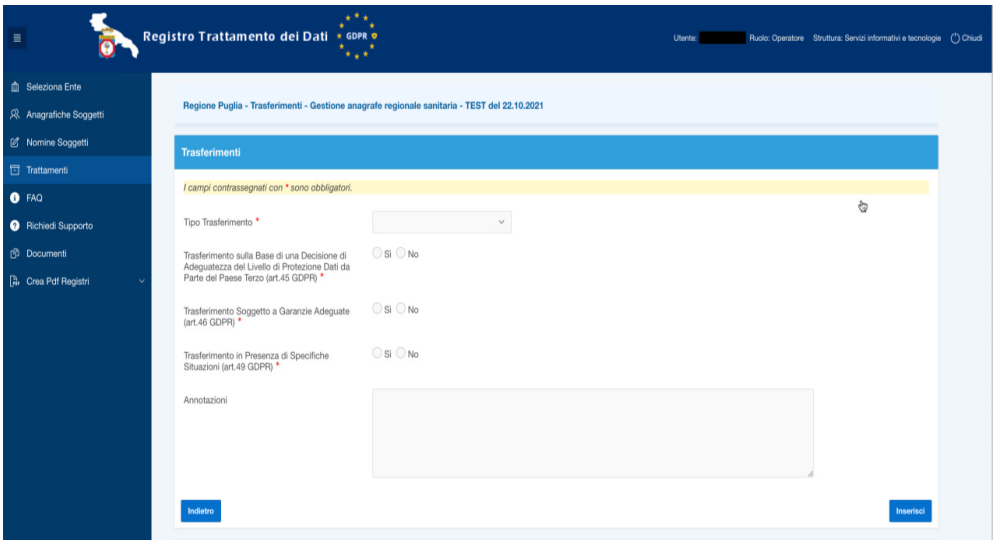
Nella schermata del Registro dedicata ai trasferimenti andrà riportata l'eventuale informazione relativa ai suddetti trasferimenti, unitamente all'indicazione relativa al Paese/i terzo/i ove i dati sono trasferiti ed alle "garanzie" adottate ai sensi del capo V del GDPR.



Per inserire un nuovo trasferimento, occorre cliccare sul pulsante **Aggiungi Trasferimento**.
Verrà richiesta a questo punto una conferma se si vuole inserire Trasferimenti di dati personali verso un paese terzo o Organizzazione Internazionale.



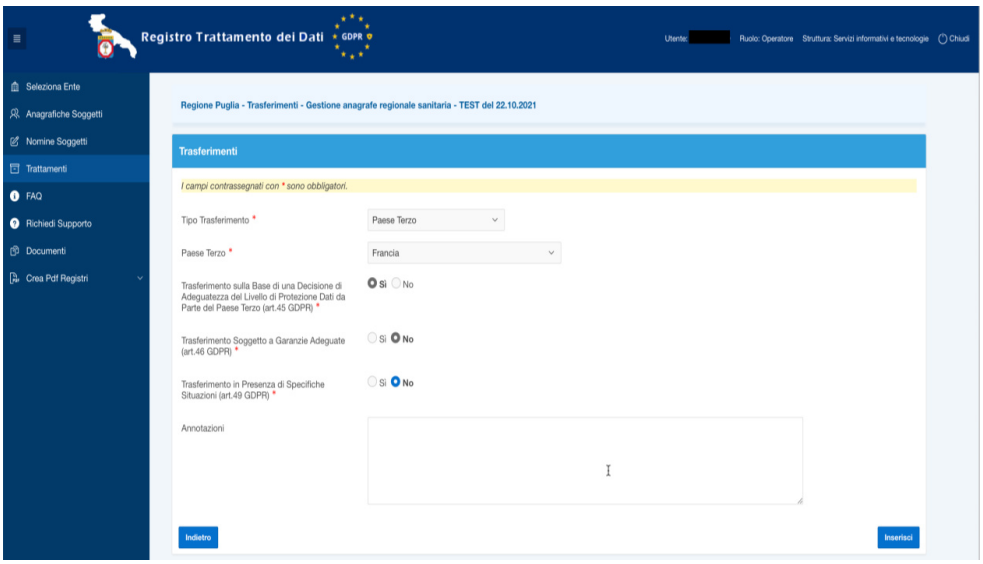
In caso di risposta positiva verrà poi presentata la pagina seguente:



Il campo **Tipo Trasferimento** permette di indicare se il trasferimento dei dati riguarda un Paese terzo o un'Organizzazione internazionale. Per entrambe le opzioni, a seguito della selezione, verrà visualizzato un ulteriore campo in cui occorrerà inserire la denominazione del Paese terzo o dell'Organizzazione destinataria del trasferimento.

Delineato il tipo di trasferimento il sistema chiede di selezionare la condizione che autorizza il trasferimento di dati personali verso paesi terzi (al di fuori dell'UE) tra quelle previste dagli artt. 45 – 49 GDPR:

- Trasferimento sulla Base di una Decisione di Adeguatezza del Livello di Protezione Dati da Parte del Paese Terzo (art. 45 GDPR);
- Trasferimento Soggetto a Garanzie Adeguate (art. 46 GDPR);
- Trasferimento in presenza di Specifiche Situazioni.

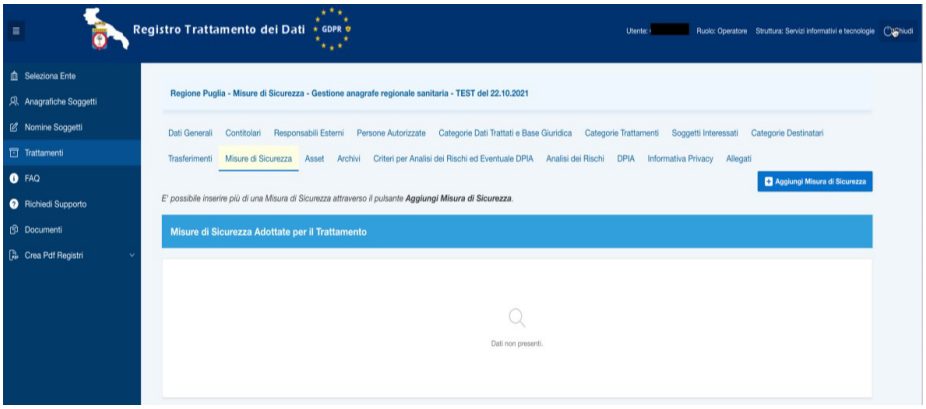


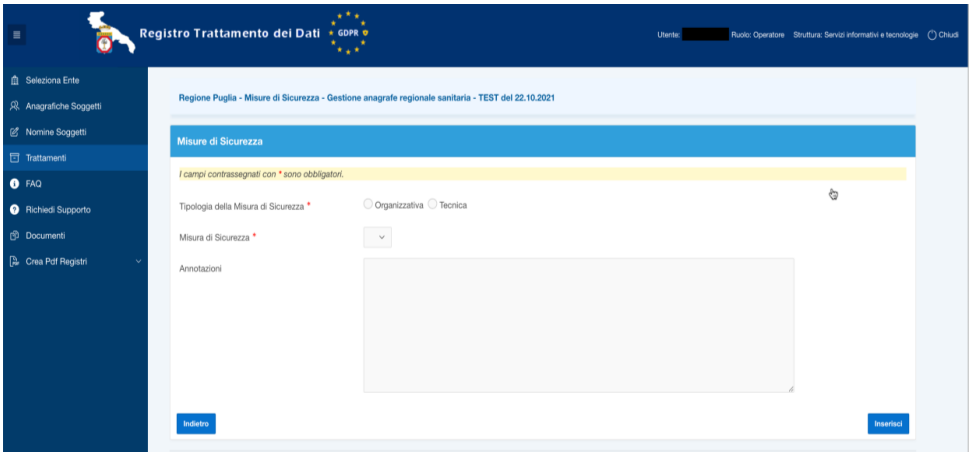
Una volta compilati i campi richiesti, occorre cliccare sul pulsante **Inserisci** per salvare i dati nel database. Il sistema segnalerà la corretta esecuzione dell'operazione richiesta tramite la visualizzazione del messaggio **Operazione eseguita correttamente**.

5.10 Misure di sicurezza

Nella schermata dedicata alle misure di sicurezza andranno indicate le misure tecniche ed organizzative, volte a garantire un livello di sicurezza adeguato al rischio, adottate dal Titolare ai sensi dell'art. 32 del GDPR nell'ambito del trattamento dati in questione, tenendo presente che l'elenco ivi riportato (pseudonimizzazione e cifratura dei dati personali; capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; capacità di ripristinare tempestivamente la disponibilità e l'accesso di dati personali in caso di incidente fisico o tecnico; procedura per testare, verificare e valutare regolarmente l'efficaci a delle misure tecniche ed organizzative; adesione ad un codice di condotta di cui all'art. 40 GDPR o ad un meccanismo di certificazione di cui all'art. 42) costituisce una lista aperta e non esaustiva, essendo rimessa al Titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente realizzate.

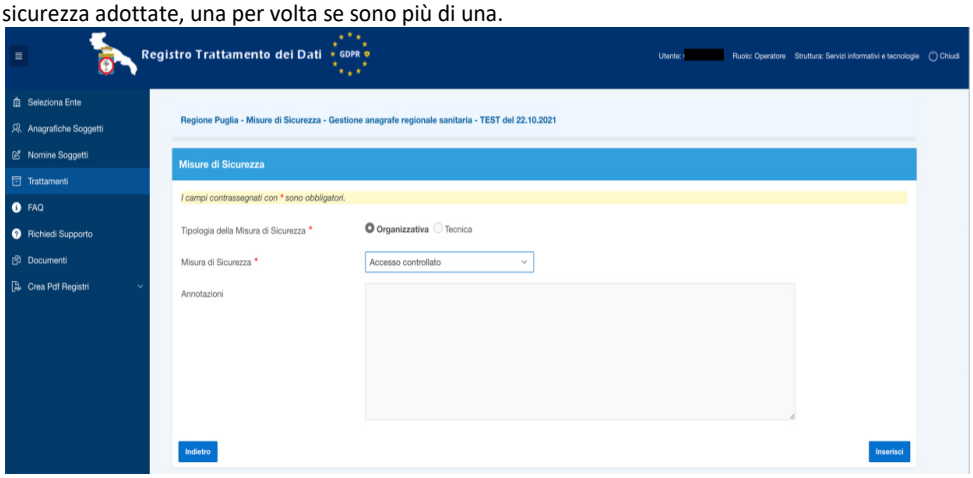
Per inserire una misura di sicurezza relativa al trattamento per cui si sta effettuando la compilazione, è necessario cliccare sul pulsante **Aggiungi Misura Sicurezza**.



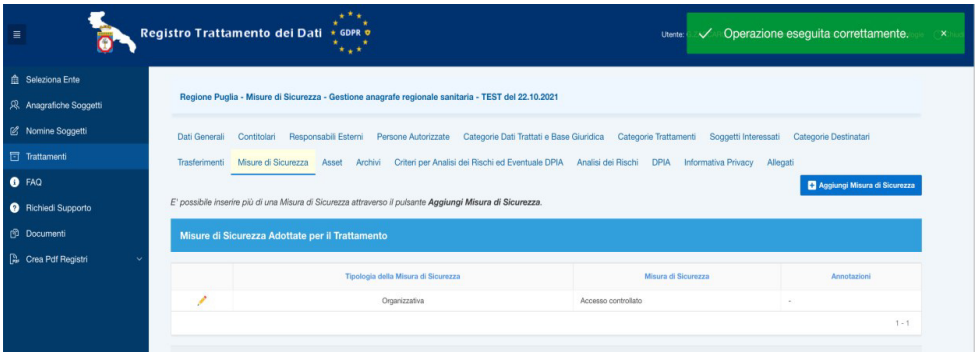


Il campo **Tipologia della Misura di Sicurezza** permette di specificare la tipologia della misura di sicurezza che si intende inserire (organizzativa o tecnica).

Una volta effettuata tale scelta è necessario selezionare - dal rispettivo menù a tendina – le misure di sicurezza adottate, una per volta se sono più di una.



Dopo aver inserito i dati richiesti, occorre cliccare sul pulsante **Inserisci** per salvare i dati nel database.



Può essere utile precisare che l'Ente Regione Puglia, con riferimento alla Sezione "Misure di Sicurezza" del RAT e nello specifico per la componente "Postazione di lavoro", applica quale standard minimo di sicurezza le misure di carattere generale di seguito elencate, riportate *di default* nel Registro - all'interno del campo "Annotazioni" - per tutti i trattamenti censiti :

1) Software di sicurezza perimetrale;
2) Log-in al PC obbligatorio con credenziali proprie dell'utente (username e password);
3) L'utente del PC non ha diritti di amministratore e quindi gli è inibita la possibilità di installare software aggiuntivo (è necessario l'intervento tecnico dell'*helpdesk*);
4) La password va obbligatoriamente modificata con cadenza periodica;
5) I dati del PC delle cartelle Desktop e Documenti sono replicati in tempo reale sui server regionali per eventuale recupero dati in caso di rottura disco.

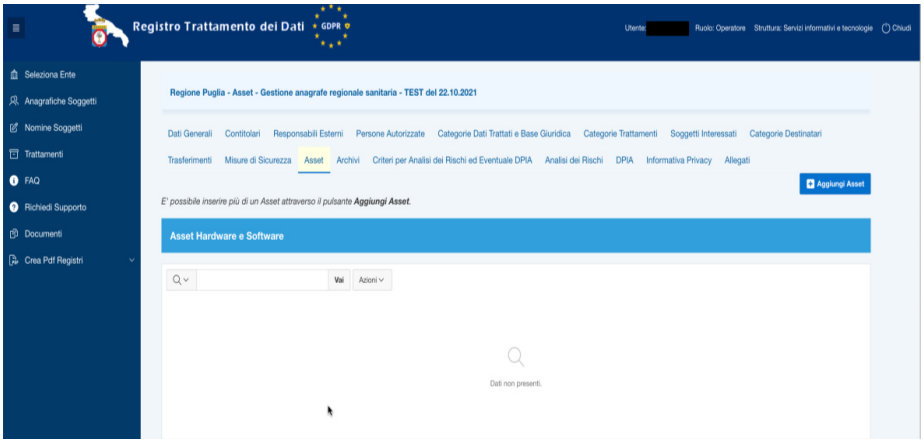
Alle suddette misure di sicurezza di carattere generale potranno essere affiancate, per i singoli trattamenti, misure di sicurezza specifiche, da indicare nel medesimo campo "Annotazioni" da parte di ciascuna Struttura interessata.

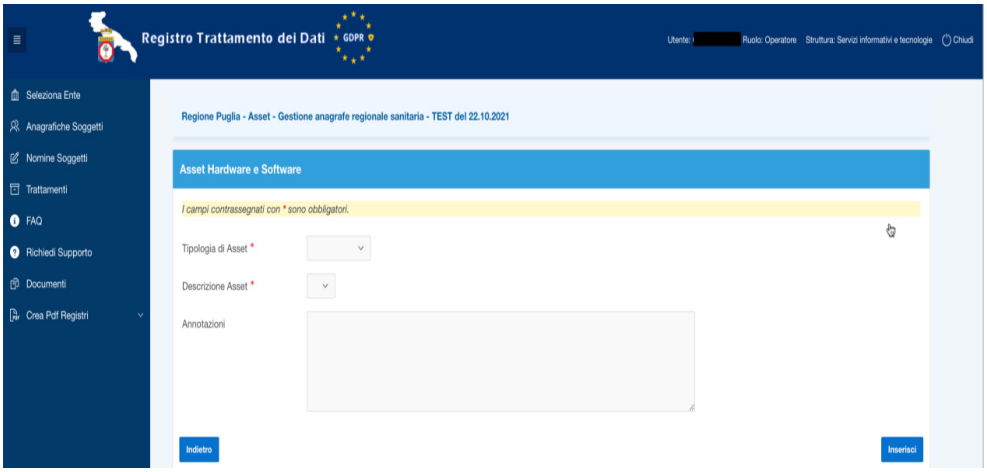
5.11 Asset utilizzati

Con il termine "*asset*" si intende, in questa sede, l'insieme degli strumenti tecnologici ed informatici – distinti in hardware e software – adoperati per trattare e conservare dati personali.

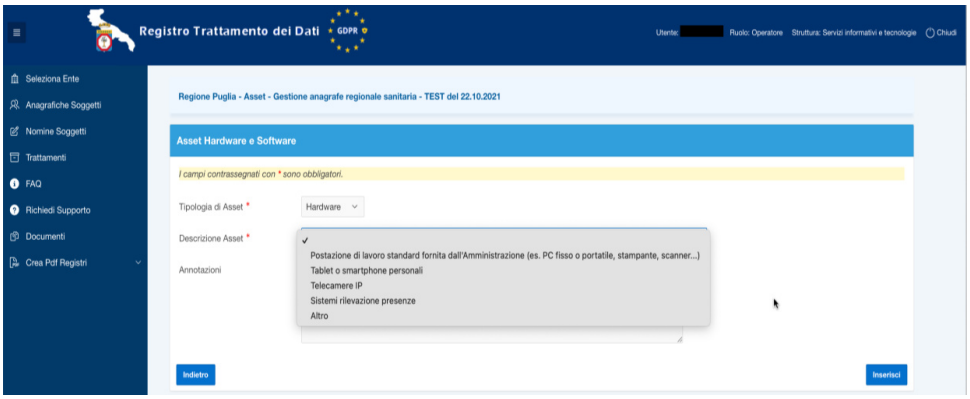
L'identificazione degli *asset* utilizzati da ciascuna Struttura organizzativa per memorizzare e gestire informazioni risulta infatti il punto di partenza per l'analisi del rischio, anche al fine di individuare le idonee misure di sicurezza a presidio dei dati personali trattati.

In questa schermata del RAT andranno indicati tutti gli asset *hardware e software* da associare al trattamento per cui si sta effettuando la compilazione.
Per inserire un nuovo Asset è necessario cliccare sul pulsante **Aggiungi Asset**.





Il campo **Tipologia di Asset** permette di specificare la tipologia di *asset* (hardware o software) che si intende associare al trattamento.
Una volta effettuata la scelta, è necessario selezionare – dal rispettivo menù a tendina – una o più opzioni, ma una per volta e con passaggi successivi.



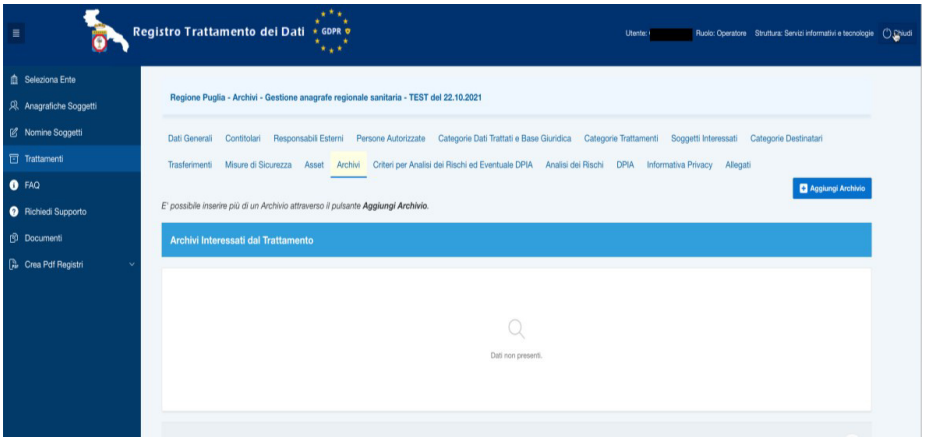
Dopo aver inserito i dati richiesti, occorre cliccare sul pulsante **Inserisci** per effettuare il salvataggio. Il sistema segnalerà la corretta esecuzione dell'operazione richiesta tramite la visualizzazione del messaggio **Operazione eseguita correttamente**.
Nel caso in cui l'*asset* che si intende inserire non fosse presente tra quelli proposti dal sistema, è sempre possibile specificarne uno nuovo selezionando l'opzione "**Altro**", e inserendo la relativa descrizione nel nuovo campo **Descrizione Altro Asset**.

5.12 Archivi

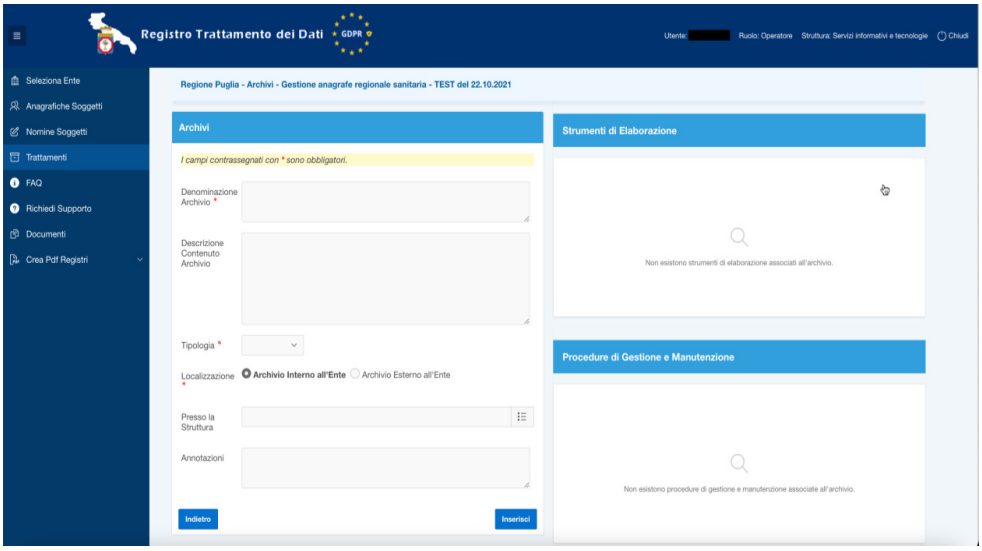
Il sistema consente di descrivere gli Archivi utilizzati per ogni singolo trattamento di dati personali.
È utile ricordare, a tal fine, che l'art. 2 del GDPR stabilisce che il Regolamento *"si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi"*.
Al successivo art. 4, par. 1, n. 6, lo stesso GDPR definisce archivio *"qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, ind*ipendentemente *dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico"*. Il considerando 15 dispone inoltre che "*al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio"*.

La definizione di archivio include dunque – come confermato dall'orientamento della più recente giurisprudenza della Corte di Giustizia Europea – anche quelle "*raccolte non automatizzate, cartacee, atte a raccogliere in modo organizzato i dati personali utilmente ad una successiva consultazione ed impiego dei dati stessi*".

Il pulsante **Aggiungi Archivio** permette di inserire le informazioni di un nuovo Archivio.



È quindi necessario compilare i campi obbligatori "Denominazione", "Tipologia" e "Localizzazione".

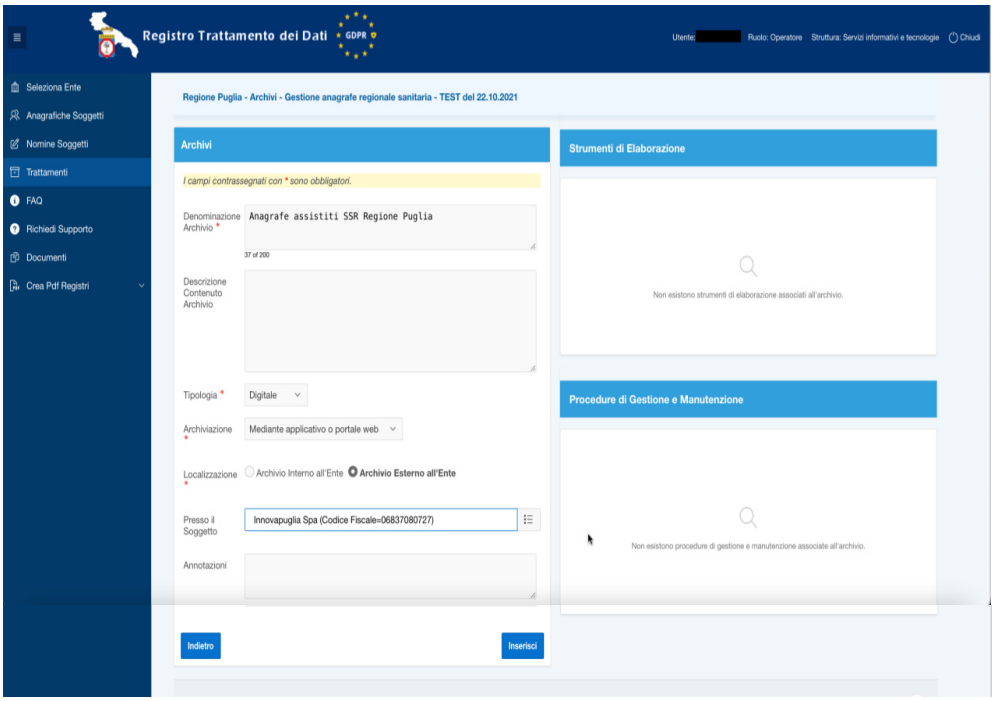


Nel campo **Denominazione Archivio** occorre impostare la denominazione dell'archivio che si intende inserire (es. Anagrafe iscritti Servizio Sanitario Regionale della Puglia).

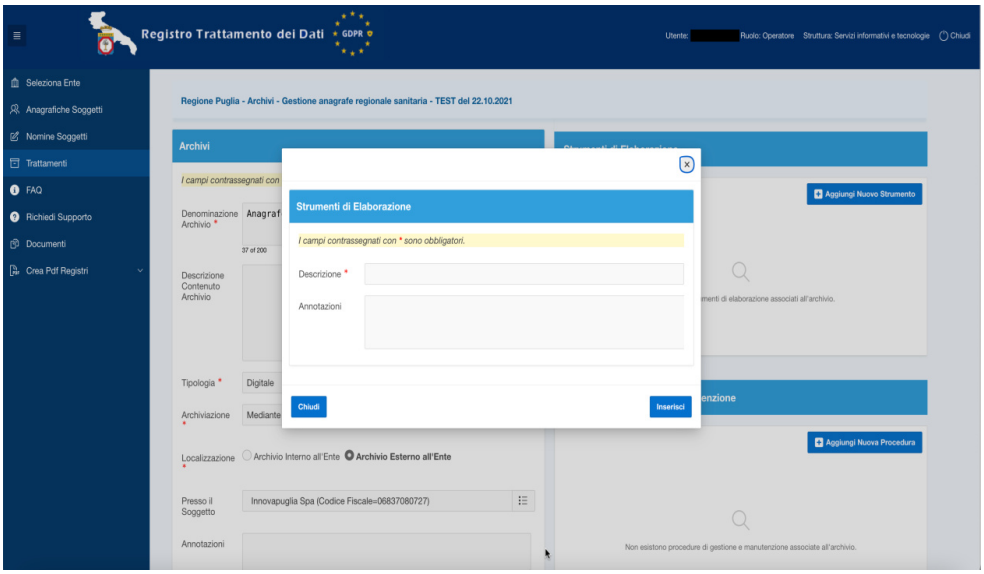
Il campo **Tipologia** permette di specificare la tipologia dell'archivio (Cartaceo, Digitale o Misto). In caso di archivio digitale o misto, è possibile specificare la tipologia di archiviazione selezionando una delle opzioni proposte dal sistema, associate al campo **Archiviazione** (Su postazione di lavoro/Mediante applicativo o portale web).

Il campo **Localizzazione** permette di specificare dove è localizzato l'archivio, se all'interno o all'esterno dell'Ente. Se si tratta di archivio interno, è possibile selezionare la Struttura regionale preso la quale è collocato; se si tratta di archivio esterno, si può indicare il data center di collocazione (es. datacenter regionale gestito dalla Società in house Innovapuglia Spa). Qualora vengano coinvolti soggetti esterni, è sempre propedeutico anagrafare e nominare gli stessi, se non già presenti nel menù a tendina.

Per salvare tutti i valori inseriti nel database e passare alla schermata successiva occorre cliccare sul pulsante **Inserisci.**

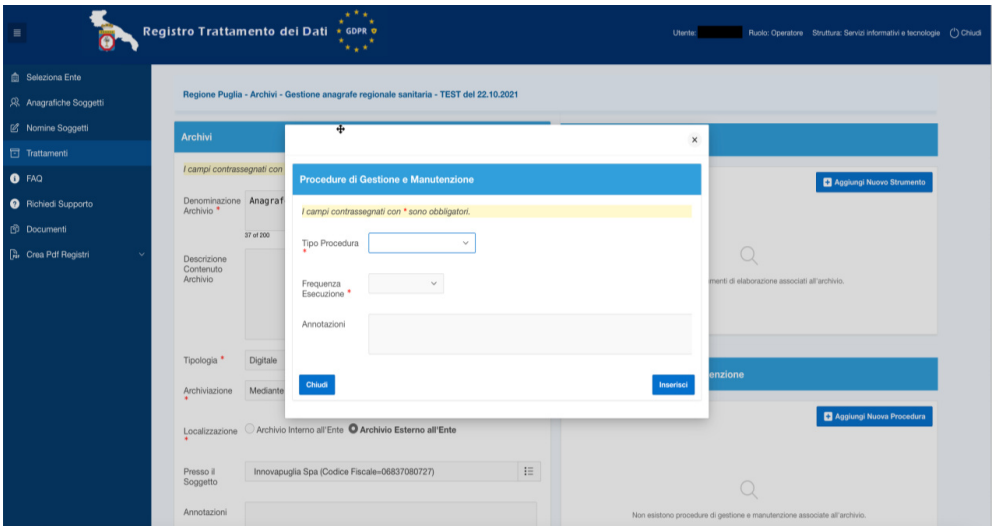


Dopo aver inserito l'archivio, è possibile procedere con la compilazione delle voci – non obbligatorie – relative a "Strumenti di Elaborazione" e "Procedure di gestione e Manutenzione" dell'archivio.
Per "Strumenti di elaborazione" si intendono gli strumenti software necessari alla gestione degli archivi. Ad esempio, nel caso di un archivio creato e gestito con Microsoft Access, per poter gestire le informazioni contenute nell'archivio è necessario avere sulla propria postazione di lavoro tale strumento: in tal caso, quindi, Microsoft Access rappresenta lo strumento di elaborazione dell'archivio. Per database più complessi, come per esempio Oracle, esistono una serie di strumenti di elaborazione all'interno della piattaforma a cui fa riferimento il database (per esempio il linguaggio standard SQL, ecc.).



Dopo aver inserito nel campo **Descrizione** le informazioni dello strumento utilizzato, occorre cliccare sul pulsante **Inserisci** per effettuare il salvataggio.

Per "Procedure di gestione e manutenzione" si intendono invece tutte le attività di gestione e manutenzione eseguite periodicamente sull'archivio al fine di tutelarne l'integrità ed operatività nel caso di malfunzionamenti o danni accidentali (*backup, restore*...).



Dopo aver impostato i campi **Tipo Procedura** e **Frequenza Esecuzione**, occorre cliccare sul pulsante **Inserisci** per salvare i valori nel database.

5.13 Criteri per analisi dei rischi ed Eventuale DPIA

Il sistema richiede, con riferimento a ciascun trattamento di dati personali, l'inserimento di informazioni relative all'analisi dei rischi ed all'eventuale necessità di procedere ad una Valutazione di Impatto del trattamento dei dati *ex* art. 35 GDPR.

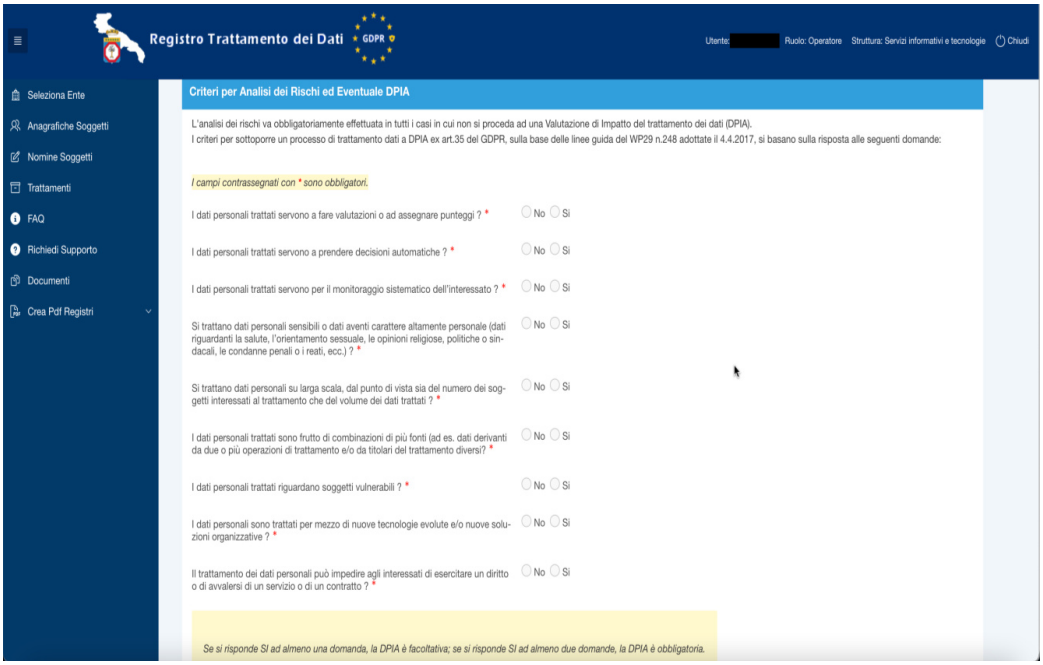
In linea generale:

- L'analisi dei rischi connessi al trattamento va obbligatoriamente effettuata.
- La valutazione d'impatto (*Data Protection Impact Assessment* - DPIA) di cui all'art. 35 del GDPR è circoscritta ai trattamenti che "*considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

Tale valutazione d'impatto-DPIA, ai sensi del suddetto art. 35, è *"richiesta, in particolare, nei seguenti casi:*

1. *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sul quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
2. *il trattamento su larga scala di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;*
3. *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

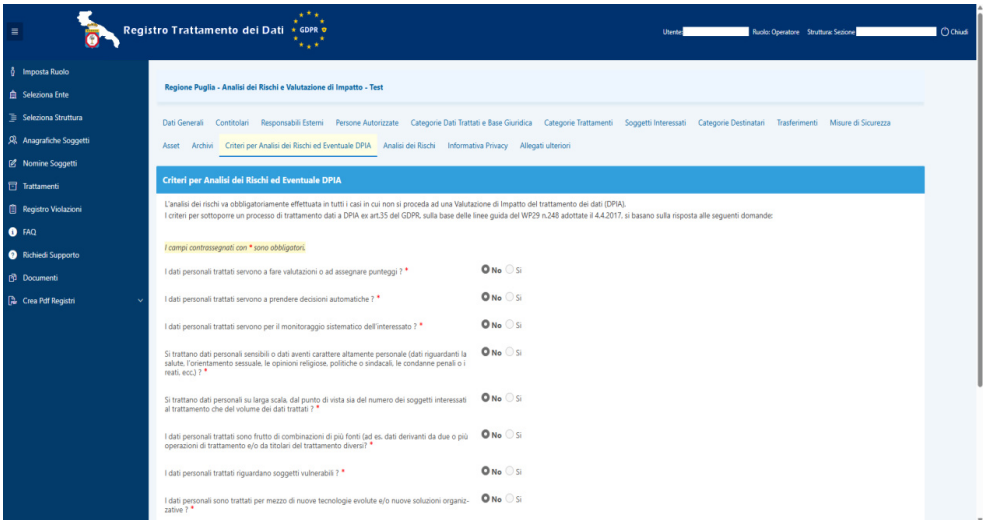
Per capire, in concreto, se un trattamento dati deve essere sottoposto o meno a DPIA ex art. 35 GDPR conviene utilizzare le indicazioni contenute nelle Linee guida del WP29 n. 248 del 4/4/2017 - cui rinvia la stessa Autorità Garante per la Privacy - che individuano a tale fine nove specifici criteri (domande), come indicato nella schermata che segue:

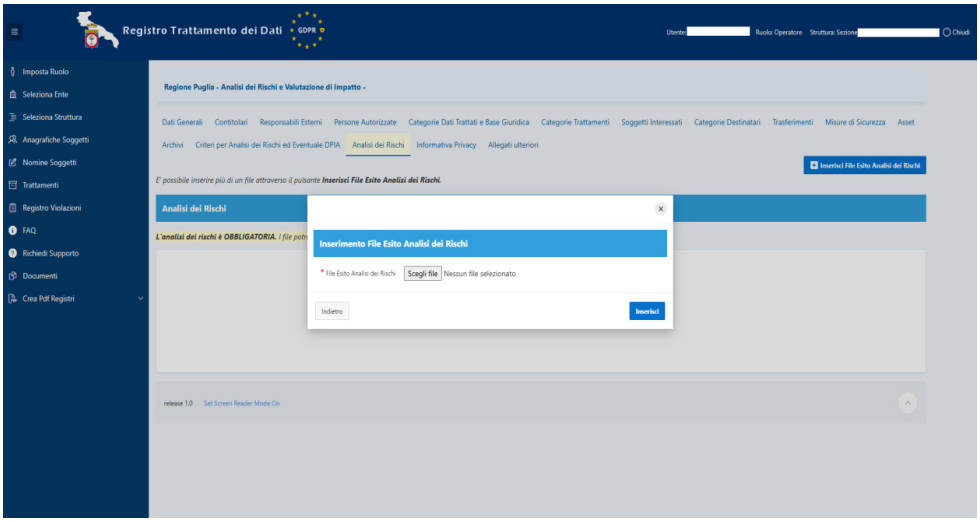


In presenza di almeno due dei criteri indicati (almeno 2 risposte SI), la valutazione di impatto DPIA è necessaria, in aggiunta alla Analisi dei rischi sempre obbligatoria; in presenza di almeno uno dei criteri indicati (almeno 1 risposta SI), la valutazione di impatto DPIA è facoltativa, in aggiunta alla Analisi dei rischi sempre obbligatoria; in assenza dei criteri indicati (tutte risposte NO) la valutazione di impatto DPIA non è necessaria e si deve procedere esclusivamente all'Analisi dei rischi.

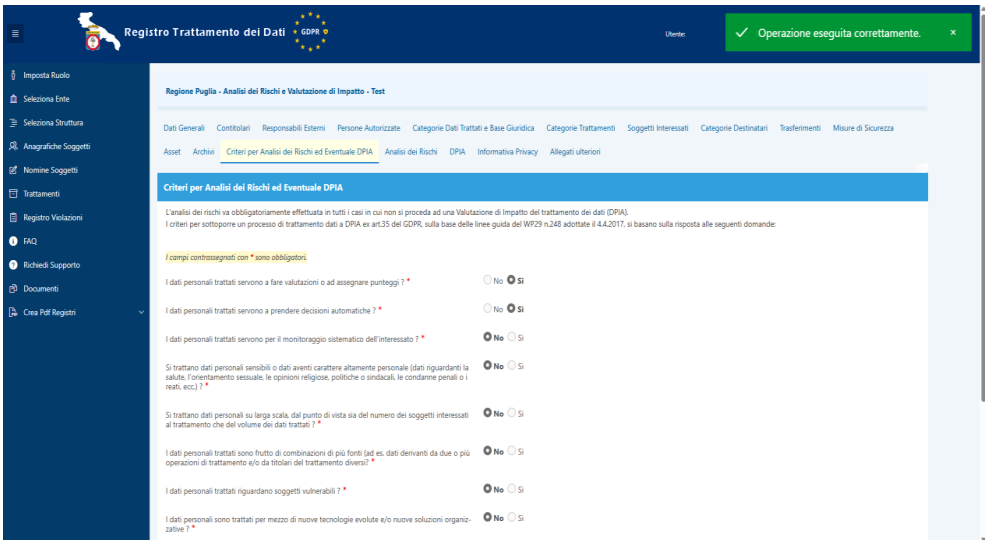
Si configurano dunque tre possibili scenari, di seguito rappresentati:
Scenario n. 1 - Se l'opzione di risposta è **NO per tutti i criteri indicati**, come nella schermata che segue, dopo aver cliccato sul pulsante **Aggiorna** per effettuare il salvataggio, si dovrà procedere

esclusivamente con l'Analisi dei rischi e si dovrà caricare il file prodotto (*File Esito Analisi dei Rischi*), dopo aver cliccato sul pulsante **Inserisci File Esito Analisi dei Rischi**.

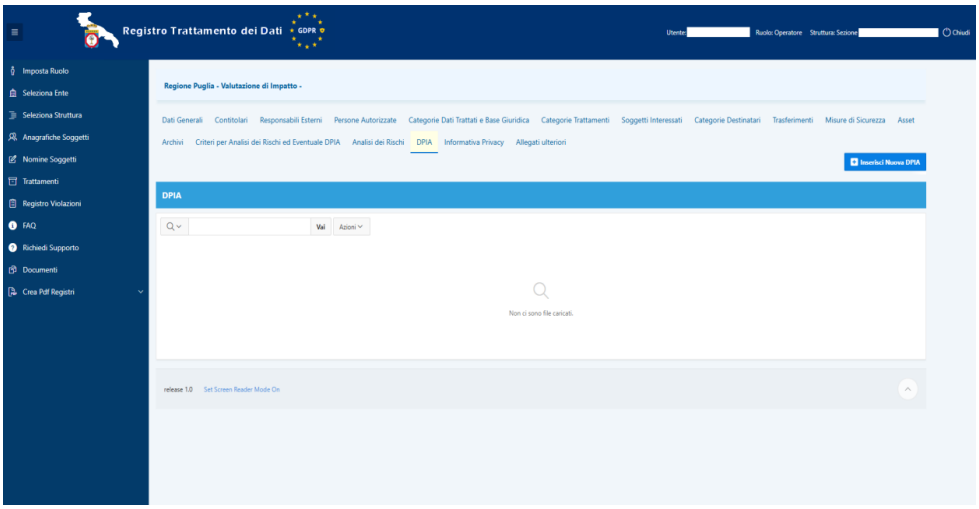


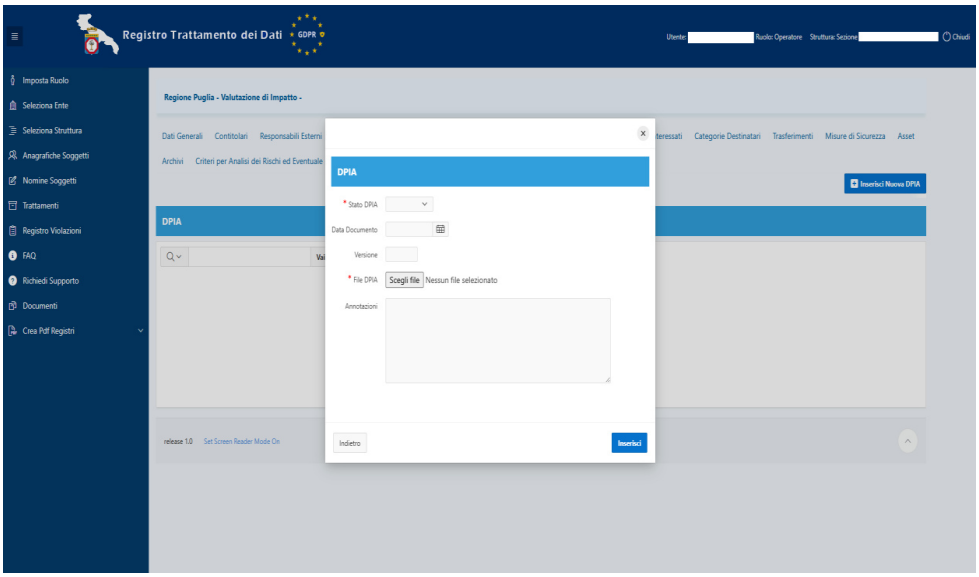


Scenario n. 2 - Se l'opzione di risposta è **SI per almeno due dei nove criteri** di cui sopra, come nella schermata che segue, dopo aver cliccato sul pulsante **Aggiorna** per effettuare il salvataggio, nel menù in alto sia la scheda "Analisi dei Rischi" che la scheda "DPIA", che in questo caso risultano entrambe obbligatorie.

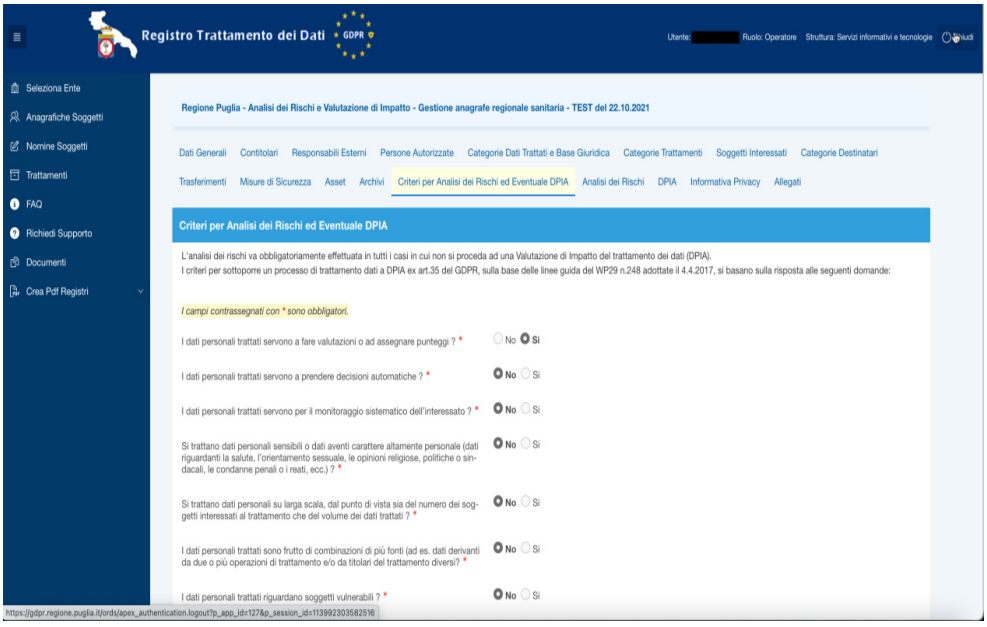


Poiché ai fini della redazione della DPIA è propedeutica l'effettuazione dell'Analisi dei Rischi, sarà necessario anche in questo caso, come per lo scenario n.1, effettuare e caricare a sistema il report dell'analisi dei rischi. Successivamente si potrà procedere alla redazione e al caricamento nell'apposita Sezione, della scheda DPIA, come rappresentato nella schermata che segue.





Scenario n. 3 - Se l'opzione di risposta è **SI per almeno uno dei nove criteri** di cui sopra, come nella schermata che segue, dopo aver cliccato sul pulsante **Aggiorna** per effettuare il salvataggio, la schermata che compare riporterà nel menù in alto sia la scheda "Analisi dei Rischi" che la scheda "DPIA", anche se in questo caso la DPIA in questo caso è facoltativa, mentre l'Analisi dei rischi resta obbligatoria.



Giova evidenziare che tanto l'Analisi dei Rischi quanto la DPIA non risultano essere degli strumenti statici, ma viceversa strumenti estremamente dinamici. Infatti, come chiarito nelle sopracitate Linee guida del WP29 n. 248 del 4/4/2017, "*qualsiasi trattamento di dati le cui condizioni di attuazione*

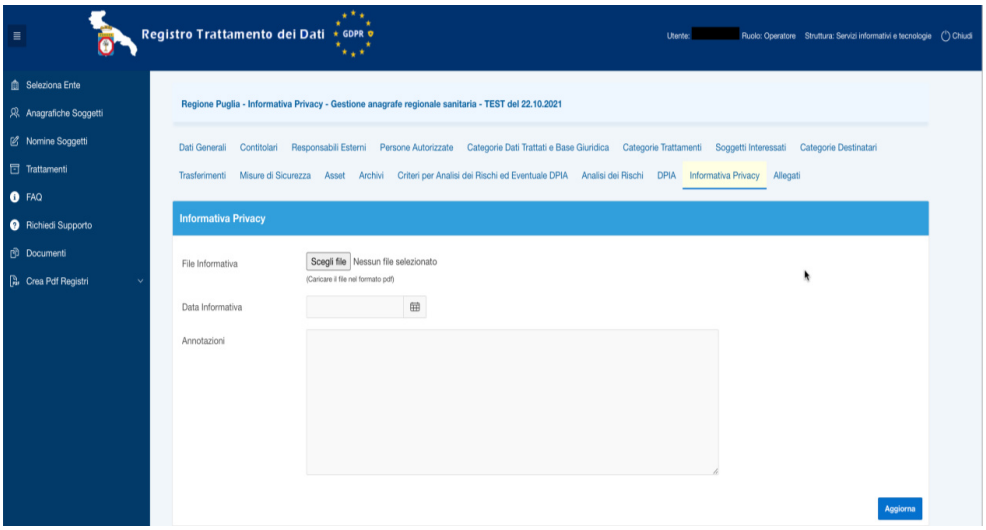
(ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'Autorità di controllo o dal Responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati". Inoltre, "*potrebbe essere richiesta una valutazione d'impatto sulla protezione dei dati in seguito a una variazione dei rischi derivante dalle operazioni di trattamento, ad esempio perché è entrata in uso una nuova tecnologia o perché i dati personali vengono utilizzati per una finalità diversa. Le operazioni di trattamento dei dati possono evolversi rapidamente e potrebbero emergere nuove vulnerabilità. Di conseguenza, va osservato che la revisione di una valutazione d'impatto sulla protezione dei dati non è utile soltanto ai fini di un miglioramento continuo, bensì anche fondamentale per mantenere il livello di protezione dei dati in un ambiente che muta nel corso del tempo. Una valutazione d'impatto sulla protezione dei dati potrebbe rendersi necessaria anche perché il contesto organizzativo o sociale per l'attività di trattamento è mutato, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione. Ciascuno di questi esempi potrebbe costituire un aspetto che porta a una variazione del rischio derivante dall'attività di trattamento interessata*".
Secondo le buone prassi, dunque, una valutazione d'impatto sulla protezione dei dati di ogni specifico trattamento va riesaminata continuamente e rivalutata con regolarità.

Avuto pertanto riguardo alla dinamicità di tali strumenti (Analisi dei Rischi e DPIA) il sistema RAT permette di inserire più versioni di analisi dei rischi e di DPIA, utilizzando – rispettivamente – il pulsante "**Inserisci File Esito Analisi dei Rischi**" oppure il pulsante "**Inserisci Nuovo DPIA**".

5.14 Informativa Privacy

Il sistema consente di registrare le informazioni relative all'Informativa privacy afferente a ciascun trattamento dati.
In questa sede è utile ricordare che per effettuare un trattamento di dati personali occorre fornire preliminarmente all'interessato alcune informazioni, per metterlo in condizione di esercitare i propri diritti ex artt. 15-22 GDPR.
I contenuti dell'Informativa sono elencati in modo tassativo negli artt. 13, par. 1, e 14, par. 1, del Regolamento stesso: in particolare, vanno sempre indicati i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), la base giuridica del trattamento, l'eventuale trasferimento di dati personali in Paesi terzi e, in caso affermativo, le caratteristiche e gli strumenti di tale trasferimento. In tutti i casi, il titolare deve specificare la propria identità, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), l'esistenza di uno o più responsabili del trattamento specificandone l'identità, i destinatari dei dati, il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, il diritto degli interessati di presentare un reclamo all'autorità di controllo.
Se i dati non sono raccolti direttamente presso l'interessato, inoltre, l'Informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.
Se il trattamento comporta processi decisionali automatizzati (inclusa la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Cliccando sulla voce di menù **Informativa Privacy**, il sistema presenta la seguente schermata:



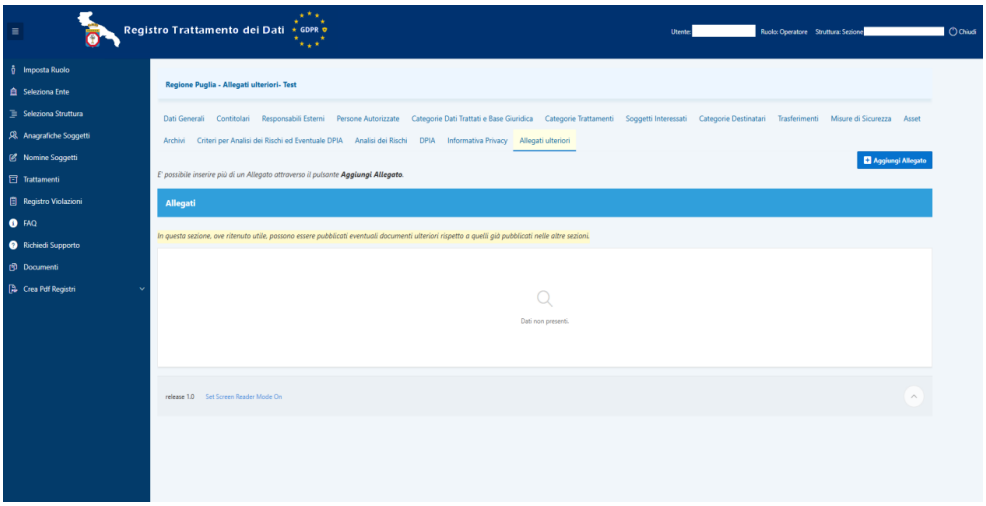
Il campo **File informativa** permette di caricare il file contenente l'informativa, selezionandolo da una cartella della propria postazione di lavoro.

Il campo **Data Informativa** permette di specificare la data a cui fa riferimento l'informativa.

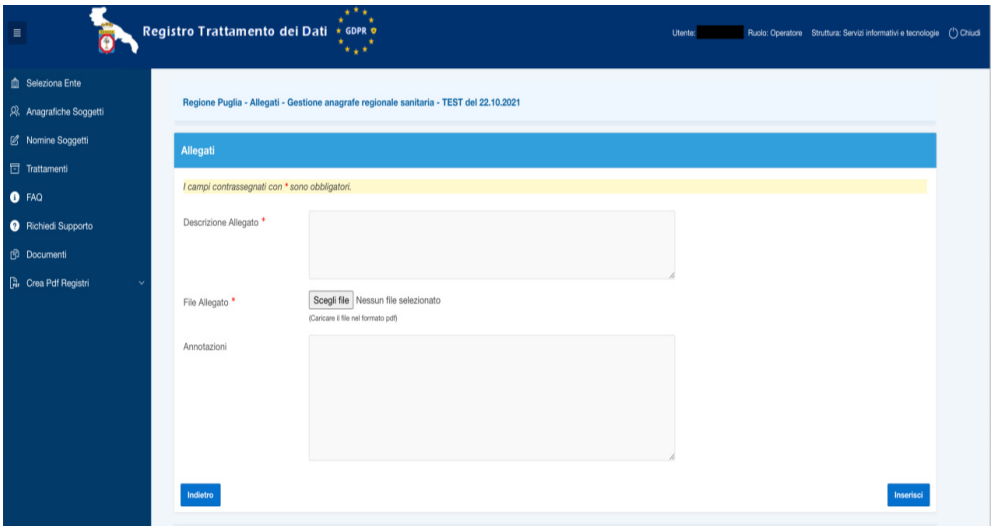
Dopo aver inserito i dati, occorre cliccare sul pulsante **Aggiorna** per effettuare il salvataggio. Il sistema segnalerà la corretta esecuzione dell'operazione richiesta tramite la visualizzazione del messaggio **Operazione eseguita correttamente**.

5.15 Allegati ulteriori

Attraverso questa schermata è possibile caricare eventuali allegati ulteriori rispetto a quelli già pubblicati nelle altre Sezioni (ad es. gli accordi *ex* artt. 26 e 28 GDPR). Anche in questo caso per inserire un documento si dovrà cliccare sul pulsante **Aggiungi Allegato**.



Dopo aver cliccato sul pulsante **Aggiungi Allegato**, il sistema presenta la seguente schermata:



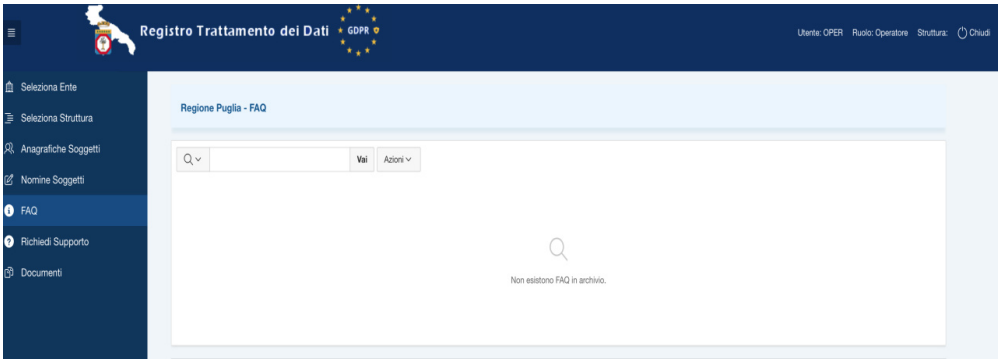
Il campo **Descrizione Allegato** permette di inserire una breve descrizione del contenuto dell'allegato.
Il campo **File Allegato** permette di caricare il file contenente l'allegato, selezionandolo da una cartella della propria postazione di lavoro.

Una volta compilati i campi obbligatori, per salvare i valori nel *database* occorre cliccare sul pulsante **Inserisci**. Il sistema segnalerà la corretta esecuzione dell'operazione richiesta tramite la visualizzazione del messaggio **Operazione eseguita correttamente**, presentando l'elenco degli allegati registrati.

6. Funzioni di supporto

6.1 FAQ

La funzione **FAQ** presente nel menù visualizzato a sinistra della *Homepage* consente all'operatore di elencare le domande più frequenti sulla procedura pervenute al Centro Servizi, con le relative risposte.
Prima di inviare una richiesta di supporto al Centro Servizi - attraverso la funzione di menù **Richiedi Supporto** - si suggerisce pertanto di visionare le FAQ.



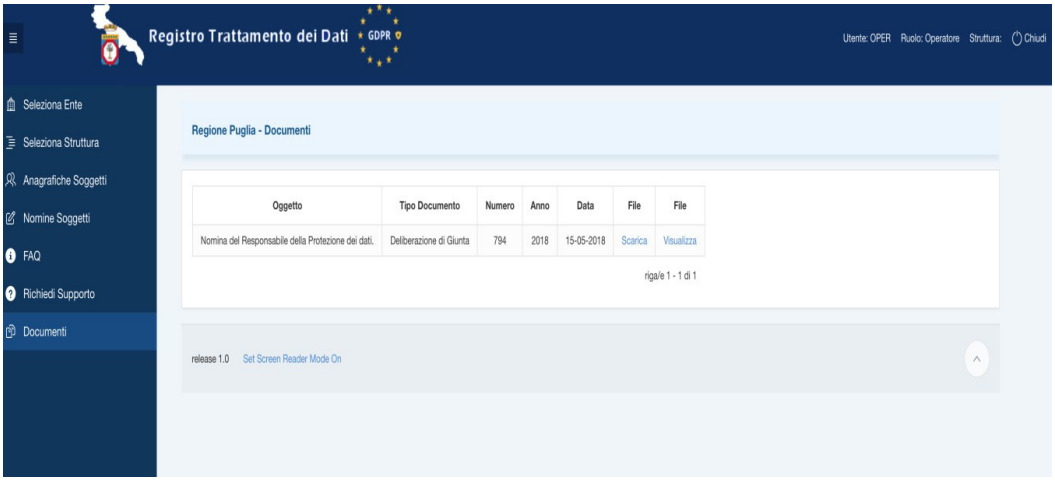
6.2 Richiedi Supporto

La funzione **Richiedi Supporto** presente nel menù visualizzato a sinistra della *Homepage* permette all'operatore di inoltrare una richiesta di supporto al Centro Servizi.
Dopo aver cliccato sulla funzione, il sistema presenterà la seguente schermata:

Per inviare la richiesta occorre inserire il testo della domanda, caricare l'eventuale file, e infine cliccare sul pulsante **Invia Richiesta**. Nel caso di eventuali anomalie, si suggerisce di allegare alla richiesta di supporto lo *screenshot* della schermata contenente il messaggio di errore ricevuto dal sistema. La risposta verrà trasmessa all'indirizzo di posta elettronica del richiedente.

6.3 Documenti

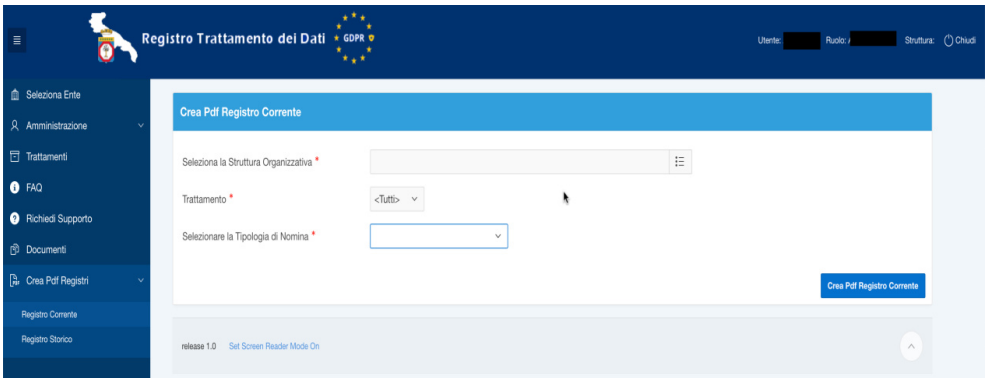
La funzione "Documenti" presente nel menù visualizzato a sinistra della *Homepage* permette di visualizzare o eventualmente scaricare i documenti di interesse generale riguardanti il Registro (es. normativa, linee guida, note informative/circolari, ecc.).



6.4 Crea Pdf Registri

6.4.1 Registro Corrente

La funzione permette di generare un file pdf contenente un singolo trattamento ovvero tutti i trattamenti della Struttura selezionata inseriti nel Registro. Per ciascuna Struttura, la lista di valori comprenderà solo i trattamenti della Struttura per cui l'operatore è autorizzato ad operare. Dopo aver cliccato sulla funzione, il sistema presenta la seguente schermata:



Per generare il pdf del Registro corrente occorre dunque impostare i campi obbligatori e cliccare sul pulsante **Crea Pdf Registro Corrente.**
Se si è abilitati ad operare su più Strutture occorre selezionare la Struttura cui afferisce il trattamento/trattamenti. Nel campo **Trattamento** è possibile specificare l'opzione "Tutti" per richiedere l'elaborazione di tutti i trattamenti afferenti ad una specifica Struttura, o in alternativa l'opzione relativa ad un determinato trattamento.

6.4.2 Registro Storico

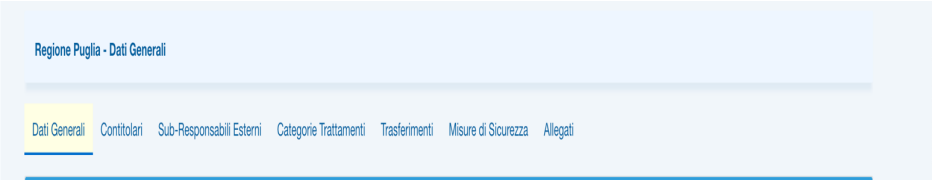
La funzione permette di generare un file pdf contenente i trattamenti della Struttura selezionata inseriti nel Registro, specificando per ogni operazione eseguita (inserimento, modifica e cancellazione) il nominativo dell'operatore che ha effettuato l'operazione e la data in cui la stessa è stata effettuata.
Per tale funzione di menù si rinvia alle considerazioni riportate per la funzione di menù "Crea Pdf Registro Corrente" in ordine alla compilazione dei campi obbligatori.

7. Trattamento dati effettuato da Regione Puglia in qualità di Responsabile del trattamento

Per ogni trattamento la cui la titolarità è posta in capo ad un soggetto esterno diverso da Regione Puglia (opzione **Titolare Dati = Altro Soggetto, con la Regione Puglia Responsabile del Trattamento**), e non sono previsti per il trattamento uno o più Contitolari (opzione **Eventuali Contitolari=NO**), il menu in alto visualizzerà le seguenti schede:

- Dati Generali
- Sub-Responsabili Esterni
- Categorie Trattamenti
- Trasferimenti
- Misure di Sicurezza
- Allegati ulteriori.

Al menu precedente si aggiunge la scheda "Contitolari", nel caso in cui – esistendo contitolari – l'opzione **Eventuali Contitolari** è impostata al valore **Si**.

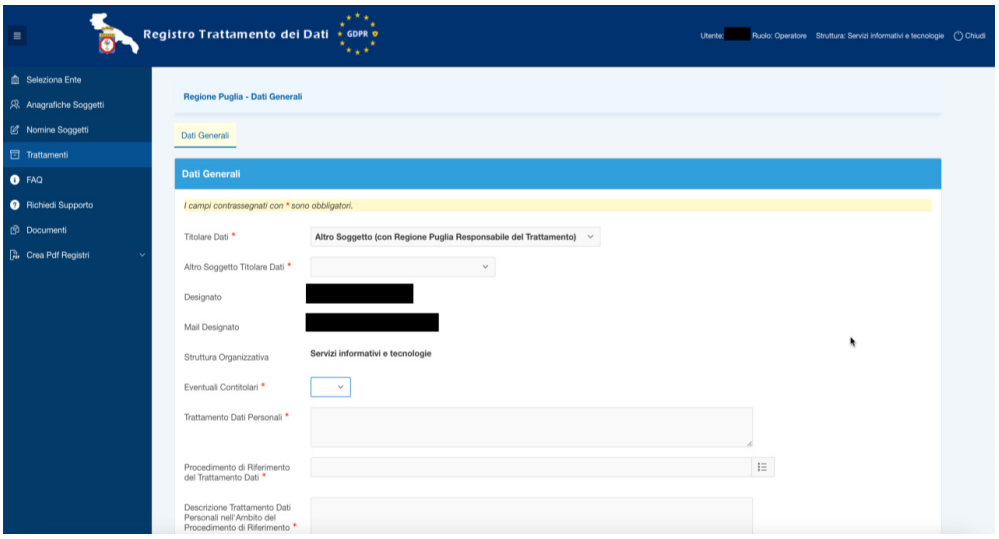


7.1. Dati generali

Se l'operatore seleziona come Titolare dati l'opzione **Altro Soggetto (con Regione Puglia Responsabile del Trattamento)**, la procedura visualizzerà il campo **Altro Soggetto Titolare Dati** per consentire, tramite apposito menù a tendina, la specificazione del soggetto esterno cui compete il ruolo di Titolare Dati.
Dopo aver selezionato dalla lista valori la denominazione del soggetto esterno, la procedura valorizzerà automaticamente i seguenti campi:

- Mail di contatto del soggetto esterno Titolare dei Dati;
- Nominativo del Responsabile Protezione Dati associato al soggetto esterno;
- Mail di contatto del Responsabile Protezione Dati del soggetto esterno.

Nel caso in cui la mail di contatto non fosse stata specificata nella relativa nomina, la procedura imposterà il campo con il valore **Non Specificata.**
Qualora nel menù a tendina del campo Altro Soggetto Titolare Dati non figuri lo specifico soggetto esterno Titolare dei dati, occorrerà registrare preliminarmente il soggetto in anagrafica.



In ordine alle modalità di compilazione degli ulteriori campi obbligatori "Eventuali Contitolari", "Trattamento Dati Personali", "Procedimento di Riferimento del Trattamento Dati", "Descrizione Trattamento nell'Ambito del procedimento di Riferimento" e "Data inizio trattamento", si rinvia alle considerazioni espresse al punto 5.1 della presente Guida, mentre il campo "Finalità" nell'ipotesi di Regione Puglia in qualità di Responsabile del trattamento è facoltativo.

7.2. Contitolari

Per la compilazione di tale schermata (opzione **Eventuali Contitolari = SI** nella precedente scheda Dati Generali) si rinvia alle indicazioni fornite al punto 5.2 della presente Guida.

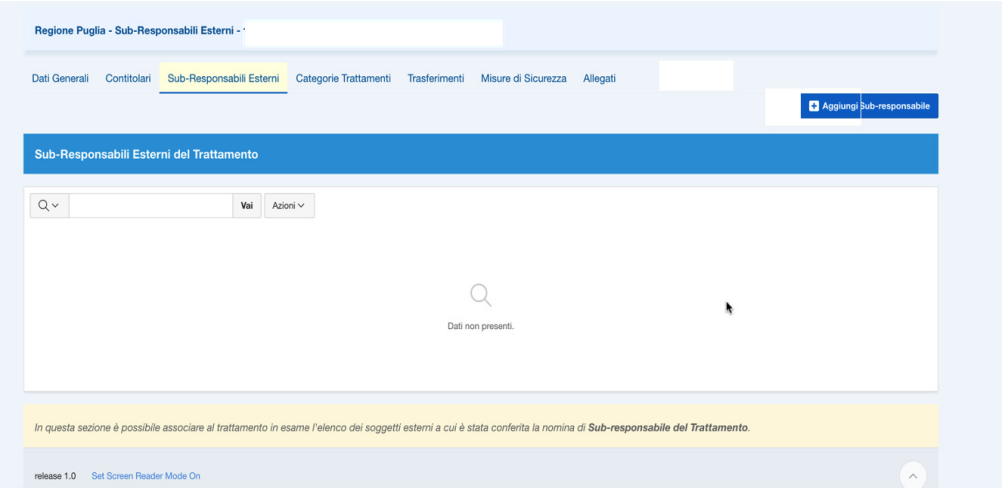
7.3. Sub-Responsabili Esterni

Il sistema consente di inserire informazioni relative ad eventuali sub-responsabili del trattamento dati.
Il sub-responsabile è una figura, eventuale, connessa a quella del Responsabile del trattamento, che interviene quando il Responsabile esternalizzi a sua volta il trattamento dei dati delegatogli dal Titolare.
In tale ipotesi, Regione Puglia (in qualità di responsabile del trattamento) dovrà:

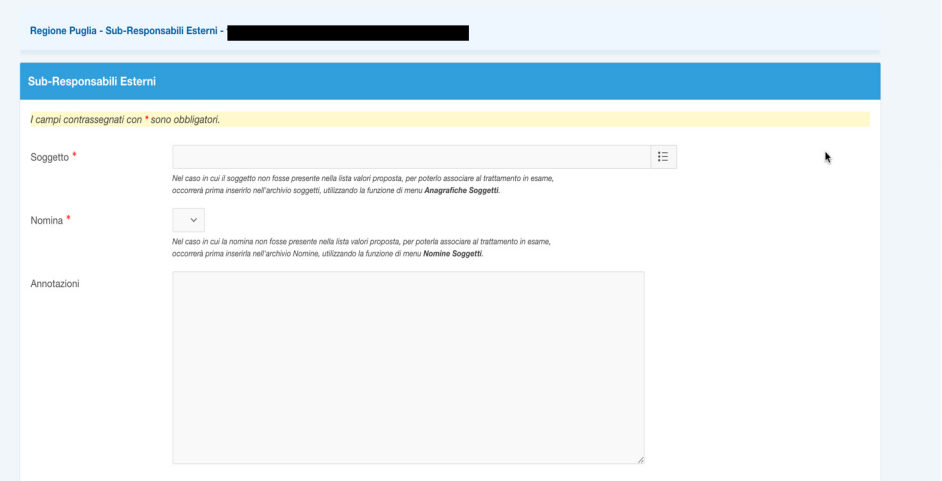
- Fornire una preventiva informazione al titolare in merito alla designazione di un sub-responsabile ed ottenere il consenso del titolare stesso;
- Redigere un accordo scritto fra responsabile e sub-responsabile che prescriva, in capo al sub-responsabile, il rispetto dei medesimi obblighi cui il responsabile è vincolato in virtù della sua nomina da parte del titolare.

Al riguardo il GDPR, all'art. 28, par. 4, contiene una specifica previsione in materia di responsabilità, disponendo che "*qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*".

Per inserire un eventuale sub-responsabile, occorre cliccare sul pulsante **Aggiungi Sub-responsabile** selezionando poi il sub-responsabile dall'apposito menù a tendina.



Qualora il soggetto sub-responsabile non figuri nella lista valori dell'apposito menù a tendina, per associarlo al trattamento in esame occorrerà preventivamente inserirlo nell'Archivio Soggetti, utilizzando la funzione di menù "**Anagrafiche Soggetti"** presente in alto a sinistra della *Home page.*
Si potrà procedere analogamente per il campo "Nomina": in tal caso, per poterlo associare al trattamento oggetto di compilazione, occorrerà prima inserirlo nell'Archivio Nomine, utilizzando la funzione di Menù "**Nomine Soggetti"** presente in alto a sinistra della *Home page*.



7.4. Categorie Trattamenti

Per tale schermata si rinvia alle indicazioni contenute al punto 5.6 della presente Guida.

7.5. Trasferimenti

Per tale schermata si rinvia alle indicazioni contenute al punto 5.9 della presente Guida.

7.6. Misure di sicurezza

Per tale schermata si rinvia alle indicazioni contenute al punto 5.10 della presente Guida.

7.7. Allegati ulteriori

Per tale schermata si rinvia alle indicazioni contenute al punto 5.15 della presente Guida.

8. Registro violazioni

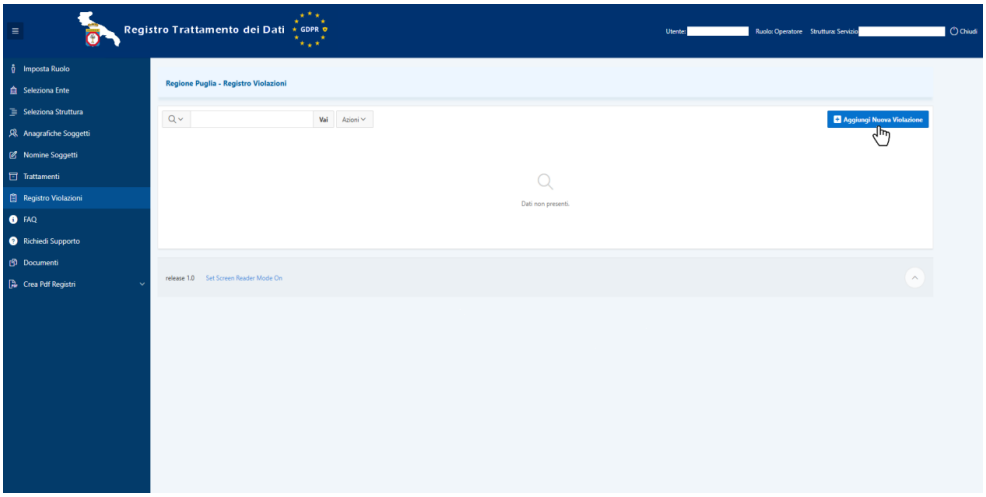
La funzione "**Registro violazioni",** presente nel menù visualizzato a sinistra della *Homepage,* consente all'operatore di inserire all'interno del medesimo Registro Violazioni – integrato nel RAT – ogni nuova violazione di dati personali che abbia interessato la Struttura di appartenenza.
Come riportato in premessa, indipendentemente dalla valutazione relativa alla necessità di procedere o meno alla notifica all'Autorità Garante (GDPD) o alla comunicazione della violazione all'interessato, ogni qualvolta si verifichi una violazione di dati personali la Regione è tenuta a documentarlo, in applicazione dell'art. 33, par. 5, del GDPR a mente del quale "*il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di controllo di verificare il rispetto del presente articolo*".
A livello generale, si rimanda alla disciplina adottata dalla Giunta Regione il materia di Gestione degli eventi di violazioni dei dati personali (c.d. *data breach*).

Al fine di inserire una violazione all'interno del "**Registro violazioni"**, dopo aver cliccato sul pulsante "Aggiungi Nuova Violazione", il sistema richiede la compilazione delle seguenti schermate:

- Dati generali
- Categoria di Soggetti Coinvolti
- Categoria di Dati Violati
- Misure di Sicurezza Adottate

- Allegati

Si specifica che solo una volta inserita la violazione attraverso la compilazione della schermata Dati generali, sarà possibile compilare le altre schermate.



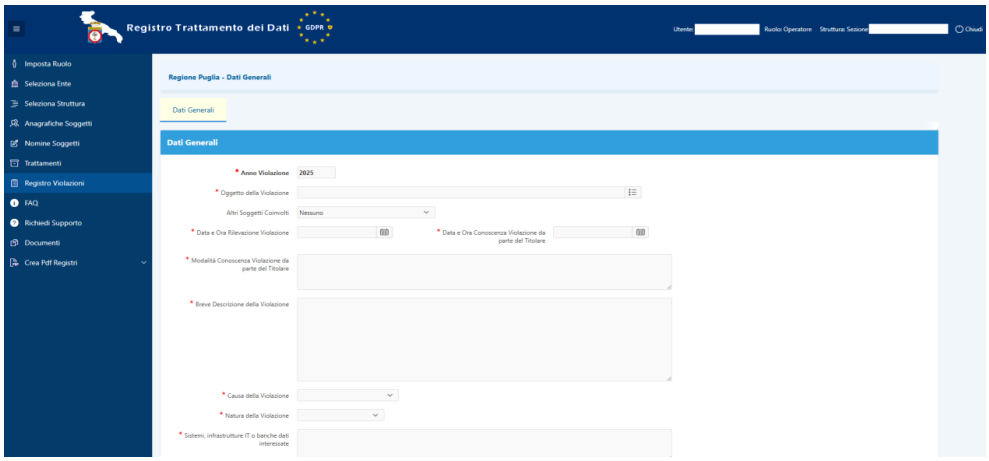
8.1 Dati Generali

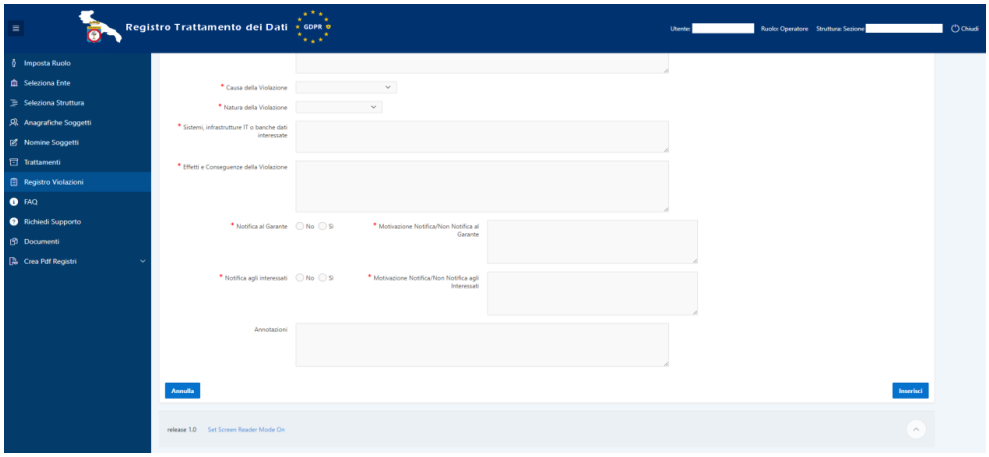
I Dati generali costituiscono l'insieme di informazioni che identificano la violazione.
In fase di inserimento di un nuova violazione, come viene raffigurato nella schermata in basso, la procedura valorizzerà automaticamente il campo **"Anno Violazione"** secondo l'anno corrente – dando comunque la possibilità all'operatore di inserire un anno differente – e richiederà obbligatoriamente la compilazione dei seguenti campi:

- Anno Violazione
- Oggetto della Violazione
- Altri Soggetti Coinvolti
- Data e Ora Rilevazione Violazione
- Data e Ora Conoscenza Violazione da parte del Titolare
- Modalità conoscenza Violazione da parte del Titolare
- Breve descrizione della Violazione
- Causa della Violazione
- Natura della Violazione
- Sistemi, infrastrutture IT o banche dati interessate
- Effetti e Conseguenze della Violazione
- Notifica al Garante
- Motivazione Notifica/Non Notifica al Garante
- Notifica agli interessati
- Motivazione Notifica/Non Notifica agli Interessati

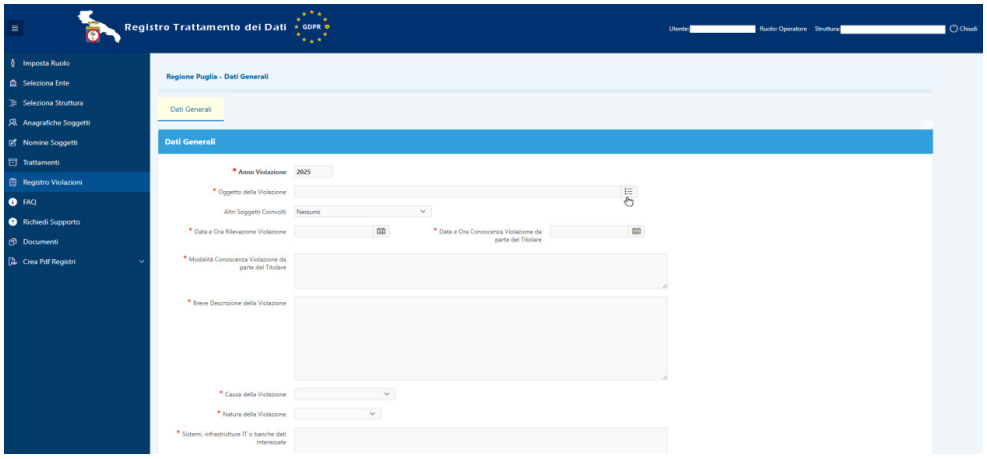
Risulterà invece facoltativa la compilazione dell'ulteriore campo:

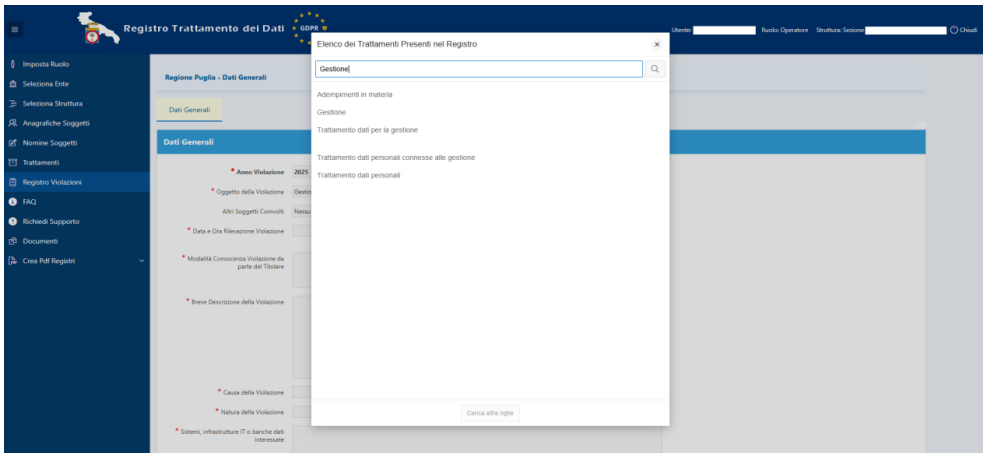
- Annotazioni





In fase di inserimento di una nuova violazione, cliccando sulla lista associata al campo **Oggetto della Violazione**, è possibile richiamare l'Elenco dei Trattamenti presenti nel Registro, al fine di individuare il trattamento – censito in precedenza attraverso la funzione **Trattamenti** – interessato dalla violazione.





Cliccando poi sull'icona elenco posta in corrispondenza del campo "**Altri Soggetti Coinvolti**", il sistema visualizza in apposito menù a tendina l'elenco di seguito proposto:

a) Nessuno
b) Responsabile del trattamento
c) Contitolare del trattamento
d) Responsabile e Contitolare del trattamento

Ciò dà evidenza della possibilità o meno del coinvolgimento nella violazione di dati di soggetti terzi (rispetto all'Ente Regione Puglia).

I due campi successivi permettono di fissare il momento temporale – rispettivamente – della rilevazione della violazione e della conoscenza da parte del Titolare/Designato della stessa.
In particolare il campo "**Data e Ora Rilevazione Violazione**" e il campo "**Data e Ora Conoscenza Violazione da parte del Titolare**" permettono l'inserimento (sia cliccando direttamente sul campo e scrivendo nello stesso, sia cliccando sull'icona raffigurante il calendario per poi scorrere fino alla data e all'ora desiderata) della data e dell'ora di rilevazione della violazione nonchè di quelle di conoscenza della violazione da parte del Titolare.
Si ricorda che il momento della violazione si riferisce al momento in cui si verifica effettivamente la compromissione dei dati personali. Il momento della conoscenza, invece, è quello in cui il Titolare/Designato viene a conoscenza dell'avvenuta violazione. Tale distinzione è fondamentale ai fini della decorrenza del termine di 72 ore previsto dal GDPR per la notifica della stessa violazione al Garante Privacy, atteso che a mente dell'art. 33 del GDPR rubricato "*Notifica di una violazione di dati personali all'autorità di controllo*", il Titolare del trattamento notifica la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza.
Proseguendo nella compilazione, il campo "**Modalità Conoscenza Violazione da parte del Titolare**" permette di fornire una breve descrizione circa la modalità con la quale è stato notiziato il Titolare della violazione in essere e il successivo campo "**Breve Descrizione della Violazione**" permette di fornire una panoramica descrittiva della stessa violazione.
Cliccando sull'icona elenco posta in corrispondenza del campo "**Causa della Violazione**", il sistema visualizza l'elenco di seguito proposto, nell'ambito del quale va selezionata un'opzione:

a) Azione intenzionale interna;
b) Azione accidentale interna;
c) Azione intenzionale esterna;
d) Azione accidentale esterna;
e) Sconosciuta.

Cliccando poi sull'icona elenco posta in corrispondenza del campo "**Natura della Violazione**", il sistema visualizza l'elenco di seguito proposto, nell'ambito del quale va selezionata un'opzione:

a) Perdita di riservatezza;
b) Perdita di integrità;
c) Perdita di disponibilità.

In ordine ai summenzionati concetti di perdita di riservatezza, perdita di integrità e perdita di disponibilità si rinvia ai contenuti della disciplina regionale in materia di gestione degli eventi di violazione dei dati personali (*data-breach*).

Il campo "**Sistemi, infrastrutture IT o banche dati interessate**" e il campo "**Effetti e Conseguenze della Violazione**" permettono di indicare, nel primo caso, il sistema, l'infrastruttura IT o la banca dati compromessa dalla violazione, e nel secondo caso gli effetti/conseguenze che tale violazione ha prodotto.

Proseguendo nella compilazione, il campo "**Notifica al Garante**" permette di indicare la decisione di comunicare o meno la violazione al Garante Privacy (No/Si), riportandone le ragioni nel prospicente campo "**Motivazione Notifica/Non Notifica al Garante**".

Se l'operatore seleziona l'opzione affermativa (Si) al campo "**Notifica al Garante**" il sistema prevede la compilazione di ulteriori campi:

- ID notifica/fascicolo assegnato dal GPDP;
- Esito notifica violazioni dati personali;
- Allegazione Provvedimento GPDP.

Il campo "**ID notifica/fascicolo assegnato dal GPDP**" permette l'inserimento dell'identificativo automaticamente attributo dal Garante *Privacy* in risposta alla segnalazione presentata, e la relativa compilazione è obbligatoria.

I campi successivi "**Esito notifica violazioni dati personali**" e "**Allegazione Provvedimento GPDP**" sono di tipo facoltativo all'atto dell'inserimento della violazione nel Registro e potranno essere integrati dalla Struttura interessata in un momento successivo, in considerazione dei tempi di risposta ed eventuale adozione provvedimenti da parte del Garante Privacy .

Il campo "**Esito notifica violazioni dati personali**" permette di selezionare, in considerazione delle varie tipologie di provvedimento che può emettere il Garante, la seguente lista di valori:

- Sanzioni;
- Ordinanze ingiuntive;
- Prescrizioni;
- Archiviazione.

Inoltre, il campo "**Allegazione Provvedimento GPDP**" permette il materiale caricamento in piattaforma del documento/provvedimento comunicato dall'Authority al Titolare del trattamento in merito all'esito della violazione riscontrata.

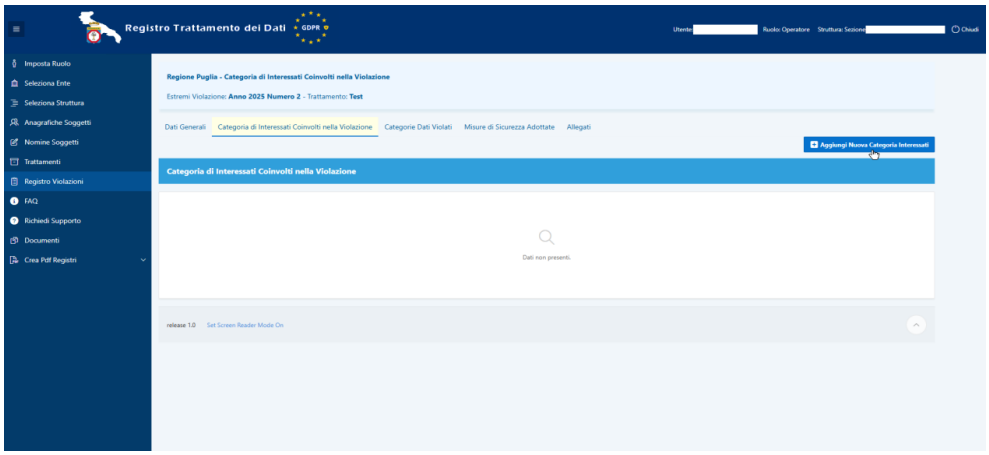
La funzione "**Notifica agli interessati"** consente di indicare la decisione di comunicare o meno la violazione all'interessato (No/Si), mentre il campo successivo "**Motivazione Notifica/Non Notifica agli Interessati**" consente di chiarire le ragioni sottese a tale scelta precedentemente espressa.

In ultimo, il campo "**Annotazioni**" permette, facoltativamente, al compilatore di annotare qualsivoglia informazione si ritenga utile segnare nel Registro delle violazioni.

Infine, cliccando sul pulsante "**Inserisci**" sarà possibile rendere definitivi tali inserimenti, che saranno confermati dall'avviso: **Operazione eseguita correttamente**.

8.2 Categoria di interessati coinvolti nella violazione

Attraverso la schermata "**Categoria di interessati coinvolti nella violazione**" è possibile inserire, cliccando sul link "Aggiungi Nuova Categoria Soggetti", i soggetti interessati nella violazione, ossia i soggetti i cui dati personali sono stati violati, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendio o altre calamità.



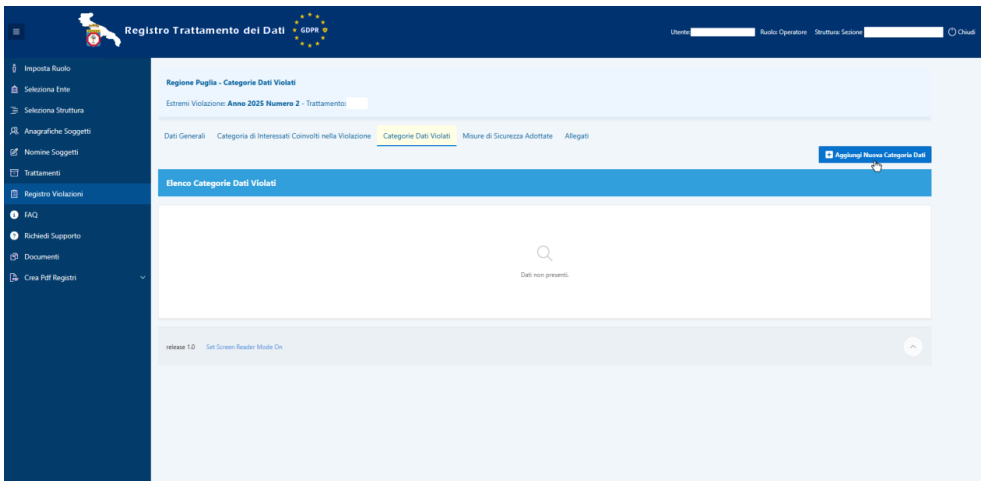
In particolare, la schermata permetterà l'inserimento delle seguenti macro-categorie di soggetti coinvolti:

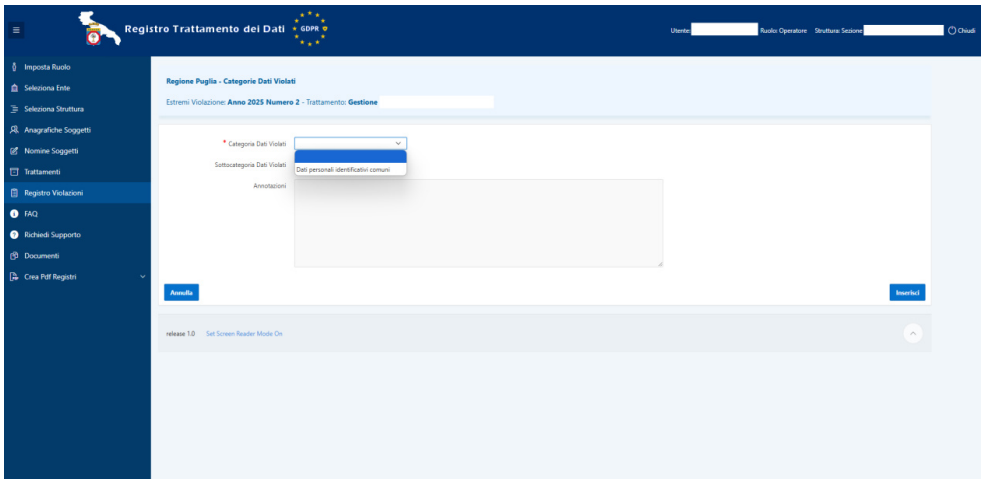
- Cittadini;
- Dipendenti.

Il campo "**Annotazioni**" permette inoltre di specificare la categoria specifica di riferimento (ad es. utenti, assistiti del servizio sanitario, beneficiari di avvisi specifici, pazienti, partecipanti ad un concorso pubblico) e di annotare qualsiasi informazione ritenuta utile.
Infine, cliccando sul pulsante "**Inserisci**" sarà possibile rendere definitive tali inserimenti, che saranno confermati dall'avviso: **Operazione eseguita correttamente**.

8.3 Categoria di Dati Violati

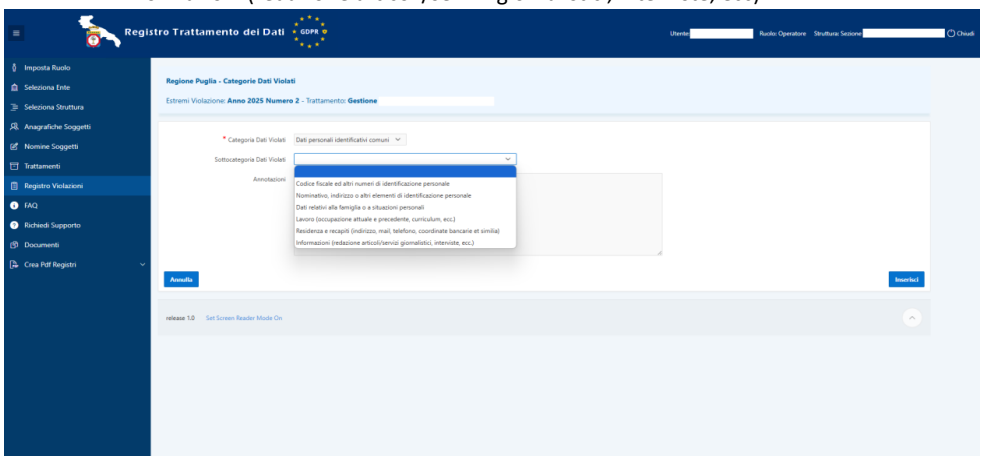
La schermata "**Categoria di Dati Violati**" consente di indicare, attraverso la funzione "Aggiungi Nuova Categoria Dati", i dati oggetto di violazione.
Si precisa che risulterà possibile inserire esclusivamente le categorie di dati già valorizzate a sistema nella relativa Sezione "Categoria Dati trattati" del RAT (a seguito del censimento dello specifico trattamento da parte della Struttura competente).





Una volta valorizzata la categoria di dati violati, risulteranno selezionabili le "**Sottocategorie Dati Violati**".
A esempio, a seguito dell'inserimento della categoria di dati violati "**Dati personali identificati comuni**" potranno essere selezionate le seguenti "**Sottocategorie Dati Violati**":

- Codice fiscale ed altri numeri di identificazione personale;
- Nominativo, indirizzo o altri elementi di identificazione personale;
- Dati relativi alla famiglia o a situazioni personali;
- Lavoro (occupazione attuale e precedente, curriculum, ecc);
- Residenza e recapiti (indirizzo, mail, telefono, coordinate bancarie *et similia*);
- Informazioni (redazione articoli/servizi giornalistici, interviste, ecc).

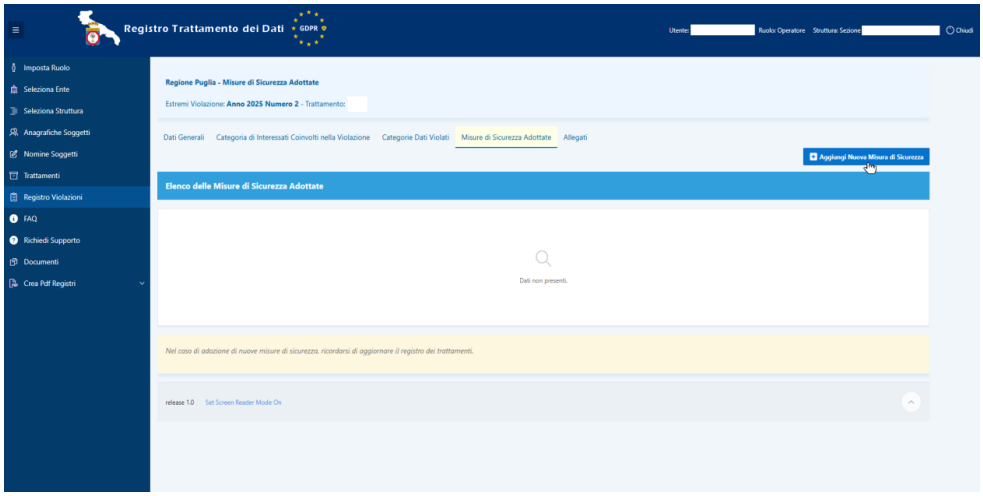


Il campo "**Annotazioni**" consente inoltre, facoltativamente, al compilatore di annotare qualsiasi informazione ritenuta utile.
Cliccando infine sul pulsante "**Inserisci**" sarà possibile rendere definitivi tali inserimenti, che saranno confermati dall'avviso: **Operazione eseguita correttamente**.

8.4 Misure di Sicurezza Adottate

Attraverso la schermata "**Misure di Sicurezza Adottate**" è possibile indicare, cliccando sul pulsante "**Nuova Misura di Sicurezza**", le misure adottate con riferimento alla violazione riscontrata.

Rammentando preliminarmente che le misure di sicurezza utili a minimizzare i danni prodotti dall'evento di *data breach* e a garantire l'effettiva protezione dei dati personali possono avere natura sia reattiva che preventiva, nel Registro andranno inserite tanto le misure di sicurezza volte a riparare/minimizzare i danni derivanti dalla violazione (evento di *data breach*) quanto le misure di sicurezza atte a potenziare per il futuro la sicurezza del trattamento dati in questione, al fine di prevenire ulteriori violazioni.



In particolare, la schermata permetterà l'inserimento – secondo una ripartizione per le distinte macroaree **CERTIFICAZIONI, MISURE ORGANIZZATIVE, MISURE TECNICHE** – delle varie **Misure di Sicurezza adottata** secondo l'elenco di seguito proposto:

CERTIFICAZIONI

- Certificazione Sistema di Gestione Qualità ISO 9001;
- Certificazione Sistema di Sicurezza delle Informazioni ISO 27001;

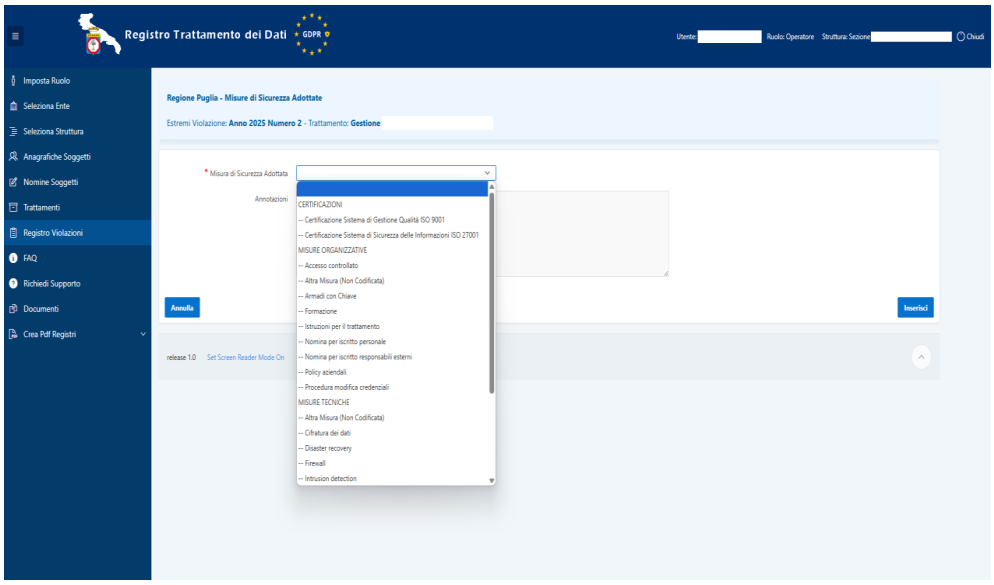
MISURE ORGANIZZATIVE

- Accesso Controllato;
- Altra Misura (Non Codificata);
- Armadi con Chiave;
- Formazione;
- Istruzioni per il trattamento;
- Nomina per iscritto personale;
- Nomina per iscritto responsabili esterni;
- *Policy* aziendale;
- Procedura modifica credenziali;

MISURE TECNICHE

- Altra Misura (Non Codificata);
- Cifratura dei dati;
- *Disaster recovery*;
- *Firewall;*
- *Intrusion detection;*
- Postazioni di lavoro;
- Antivirus;
- Separazione;
- Sistemi informativi;

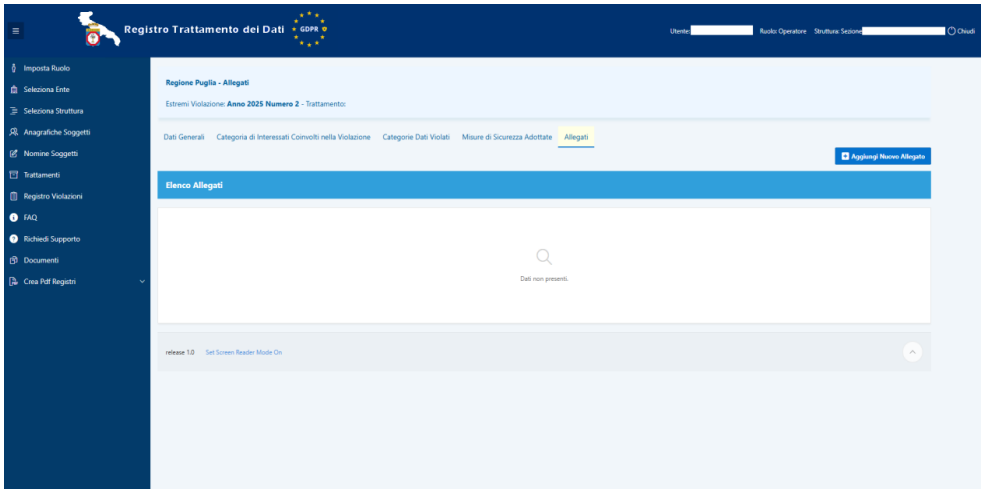
- Autenticazione;
- Autorizzazione;
- *Business Continuity;*
- *Vulnerability assessment/penetretion test*.



Il campo "**Annotazioni**" permette inoltre , facoltativamente, al compilatore di annotare qualsiasi informazione ritenuta utile.

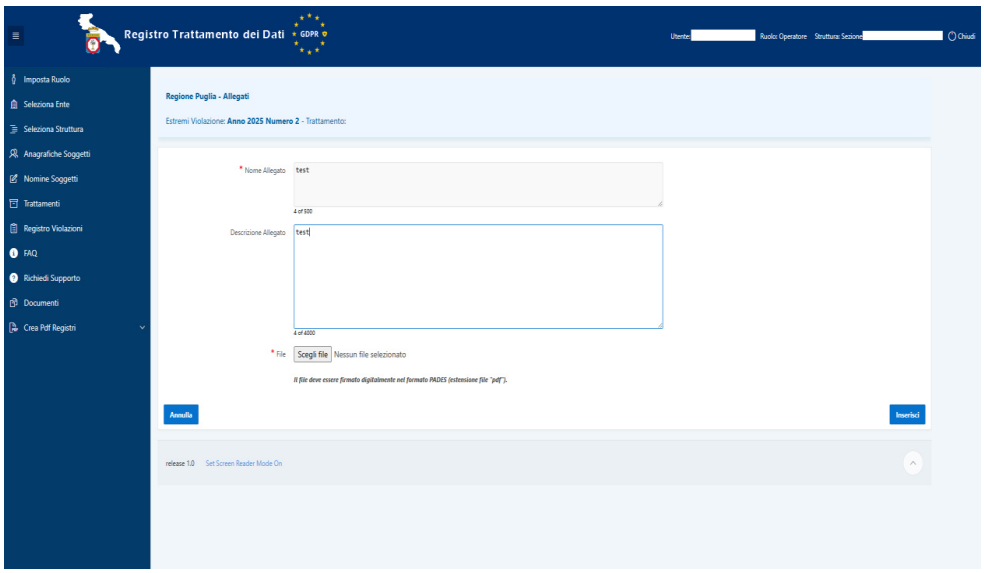
8.5 Allegati

Attraverso la schermata "**Allegati**" è possibile inserire, cliccando sul pulsante "**Aggiungi Nuovo Allegato**", eventuali documenti ritenuti utili afferenti la violazione oggetto di registrazione.



In particolare, la schermata consente l'inserimento del "**Nome Allegato**", una breve descrizione (facoltativa) del contenuto del documento in corso di allegazione all'interno del campo "**Descrizione**

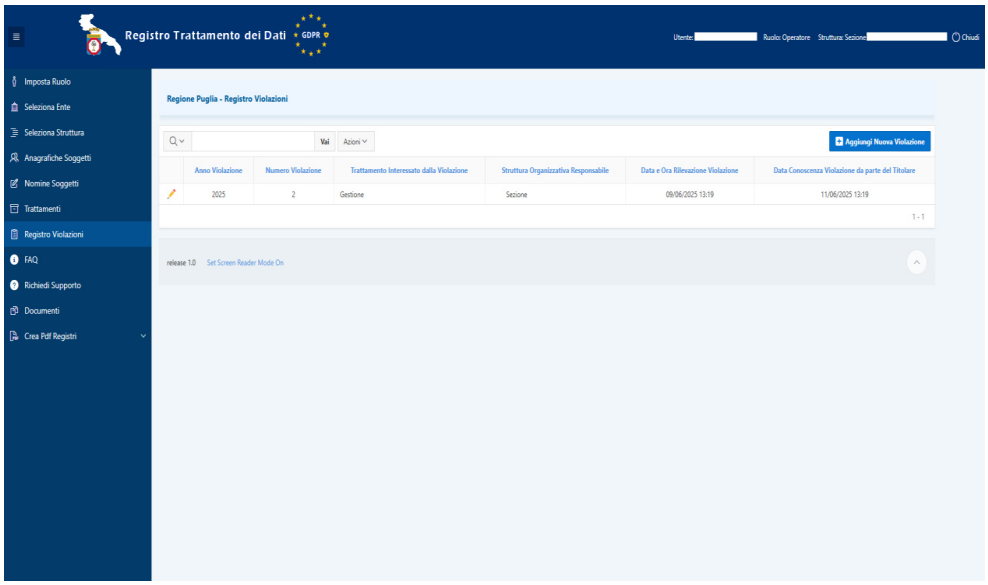
Allegato", ed il caricamento del documento tramite il pulsante "**Scegli file",** avendo cura di verificare che quest'ultimo possegga un estensione .pdf e risulti firmato digitalmente nel formato PADES.



Cliccando poi sul pulsante "**Inserisci**" sarà possibile rendere definitivi tali inserimenti, che saranno confermati dall'avviso: **Operazione eseguita correttamente**.

Una volta completata la registrazione della violazione il sistema restituisce automaticamente il numero della violazione. Tale numero sarà progressivo all'interno di ciascun anno solare.

L'operatore, al termine del corretto inserimento della violazione, potrà visualizzare all'interno della schermata generale "**Registro Violazioni**" l'elenco delle violazioni inserite nel Registro da parte della Struttura per cui l'operatore stesso risulta autorizzato.



La visualizzazione integrale della suddetta schermata "**Registro Violazioni**", con l'elenco costantemente aggiornato di tutte le violazioni inserite nel Registro da parte delle singole Strutture/Designati al trattamento, è affidata al RPD della Regione Puglia ed alla relativa Struttura di supporto.