SICURWEB

SICURWEB

SOFTWARE - RICERCA - E-LEARNING

INFOTEL®

SISTEMI SOFTWARE

SINCE 1998

GDPRIVACY SOFTWARE

Manuale d'uso

Autore	Cod. Sw	N.ro Rev.	Data
Infotel Sistemi	01	2	04/06/2019

INDICE

INDICE 1
Capitolo 1 INTRODUZIONE 2
1.1 SCHEMA DEL FLUSSO DEL PRIVACY GDPR SOFTWARE 3
1.2 CONCETTI GENERALI 4
1.3 INSERIMENTO UNITÀ ORGANIZZATIVE 4
1.4 INSERIMENTO RISORSE UMANE 5
Capitolo 2 MODULO PRIVACY 6
2.1 ARCHIVI 7
2.2 ANAGRAFICA 7
2.3 STAMPE 9
2.4 HOME 10
2.4.1. CODICI E CERTIFICAZIONI 10
2.4.2. TRATTAMENTI 11
2.4.2.1. CREAZIONE DI UN NUOVO TRATTAMENTO 12
2.4.2.2. STAMPA CONTRATTO DI NOMINA DEL RESPONSABILE TRATTAMENTO O DPO/RPD 16
2.4.3. CONSERVAZIONE DEI DATI 17
2.4.4. SOGGETTI AUTORIZZATI 17
2.4.5. ASSET 19
2.4.5.1. CREAZIONE DI UN NUOVO ASSET 20
2.4.6. REGISTRO TRATTAMENTI 22
2.5 GESTIONE SCADENZE 24
Capitolo 3 SEZIONE D.P.I.A. 25
3.1 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – INTRODUZIONE AL NUOVO REGOLAMENTO EUROPEO GDPR 25
3.2 SCHEMA DI FLUSSO DI UNA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI 26
3.3 METODOLOGIA USATA PER LA VALUTAZIONE DI IMPATTO 27
3.4 ACCESSO ALLA D.P.I.A. 27
3.4.1. CREAZIONE DI UNA NUOVA DPIA 28

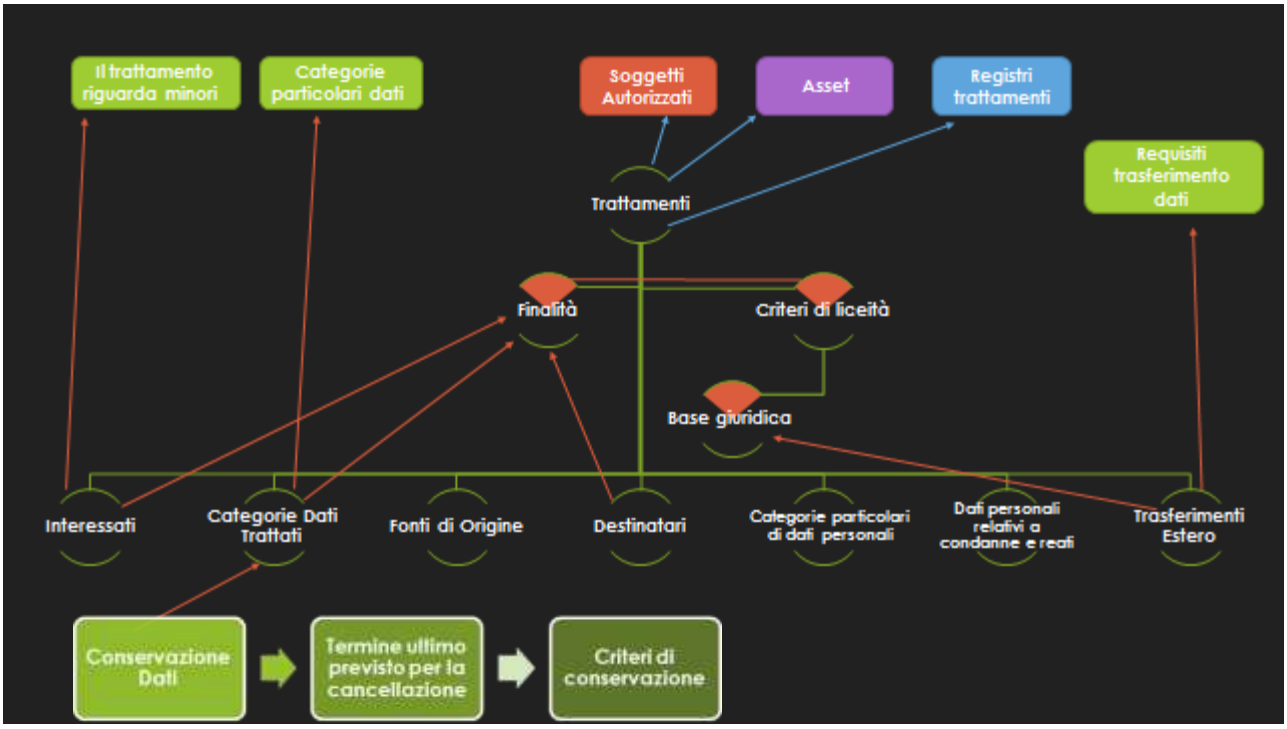
Capitolo 1 INTRODUZIONE

Privacy GDPR è un *software web*, per gestire gli adempimenti richiesti dal Regolamento Europeo 2016/679. **Privacy GDPR** permette a **Consulenti Privacy, Aziende, DPO e Enti Pubblici,** di redigere e tenere aggiornato il registro dei trattamenti per l'attuazione concreta del principio di accountability introdotto dal GDPR.

Con GDPRivacy puoi:

Inserire il Titolare del Trattamento
Inserire anagrafiche sia per interni che esterni
Inserire i trattamenti
Associare trattamenti a soggetti interni e a responsabili esterni
Elaborare il registro dei trattamenti
Gestire le scadenze ed effettuare Audit pianificati
Individuare gli Asset (Applicazioni, Database, Archivi che contengono dati personali)
Stampare le informative e raccolte al consenso per ogni categoria di interessati
Elaborare la D.P.I.A. (*valutazione di impatto sulla protezione dei dati*)
Nominare i responsabili esterni del trattamento
Nominare i D.P.O.
Designare i soggetti autorizzati

1.1 SCHEMA DEL FLUSSO DEL PRIVACY GDPR SOFTWARE



STAMPE GENERATE DAL SISTEMA

1.2 CONCETTI GENERALI

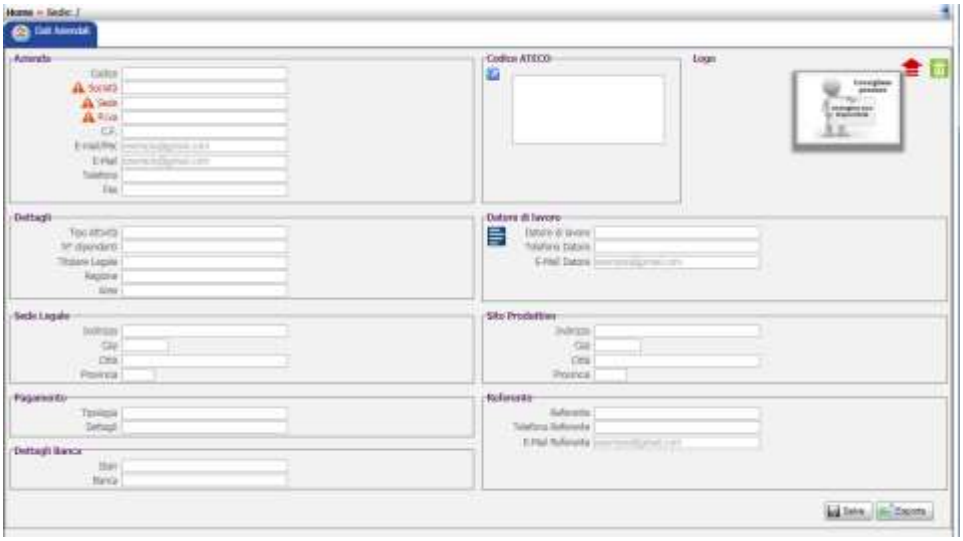
Effettuare l'accesso, tramite la login, all'indirizzo del proprio sistema, digitando l'Username e la Password.
Gli utenti amministratori hanno visibilità su tutte le funzioni e su tutte le aziende/sedi inserite.
Dopo aver effettuato l'accesso al sistema, si accede al Back Office dell'applicativo, caratterizzato dalla tabella contenente le aziende/sedi/unità produttive inserite, dalla barra dei menù e dalla barra di stato.

Per l'utilizzo del Back Office si rimanda al manuale completo di SICURWEB:
https://www.sgslweb.it/wp-content/uploads/file/Manuale_SicurWEB.pdf

1.3 INSERIMENTO UNITÀ ORGANIZZATIVE

Il primo passo è quello di creare l'**anagrafica** delle **UNITÀ ORGANIZZATIVE** su cui vanno effettuati i trattamenti dei dati personali: per fare ciò procedere attraverso il comando in alto a sinistra che aprirà un popup contenente le seguenti voci:

Selezionando l'icona Nuova Unità Organizzativa, si apre la sezione per creare una nuova azienda, come mostrato di seguito:



Compilare i campi, inserendo i dati relativi all'unità organizzativa che si vuole inserire, e salvare i dati appena inseriti con il comando Salva.

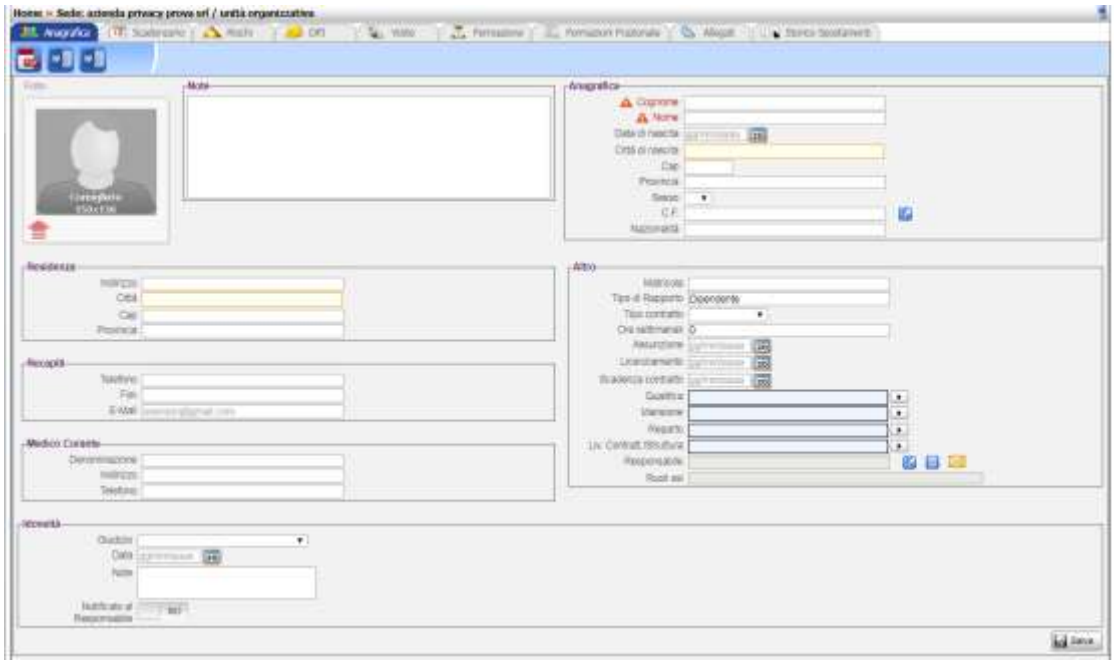
Per tornare alla pagina iniziale, utilizzare la barra di navigazione in alto a sinistra, cliccando su Home. Tale barra sarà visibile in altre sezioni del sistema.

Per ogni unità organizzativa creata, il sistema inserisce una riga nella schermata Home. Per lavorare, sulla singola unità organizzativa, selezionare la riga corrispondente.

1.4 INSERIMENTO RISORSE UMANE

Il secondo passo è quello di inserire le risorse umane attraverso la creazione delle anagrafiche. Per entrare nella sezione dei dipendenti, selezionare l'azienda inserita nel back office e cliccare, dalla colonna accessi posta a destra, la voce Risorse Umane:

Si accede così alla sezione dei dipendenti, dalla quale è possibile inserire le anagrafiche dei dipendenti.



Per maggiori dettagli **visitare la seguente pagina web:**
https://www.sgslweb.it/wp-content/uploads/file/Manuale_SicurWEB.pdf

Capitolo 2 MODULO PRIVACY

Inserita l'unità organizzativa e le rispettive risorse umane, si procede accedendo al modulo della privacy.
A tale scopo, dalla pagina Home, selezionare l'azienda su cui si vuole andare a gestire la privacy e, dalla colonna Accessi, selezionare il comando Privacy:

Si passa così alla sezione relativa la privacy.

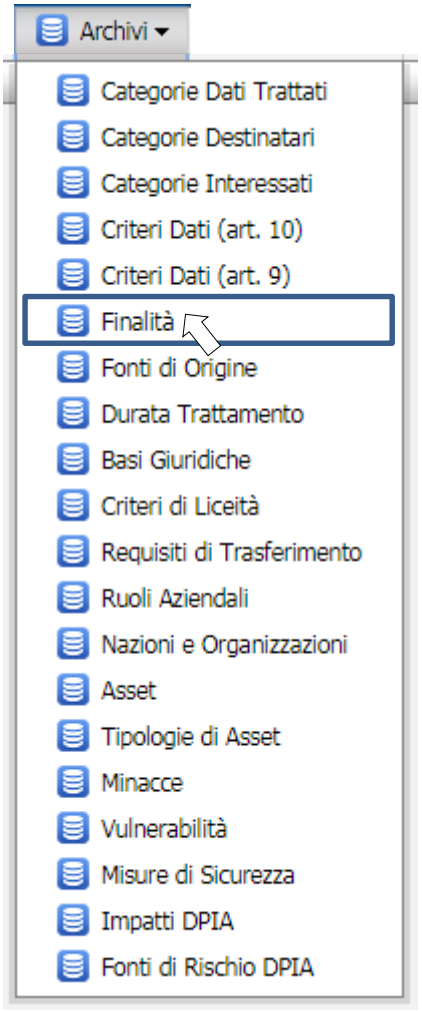
CARATTERISTICHE PRINCIPALI

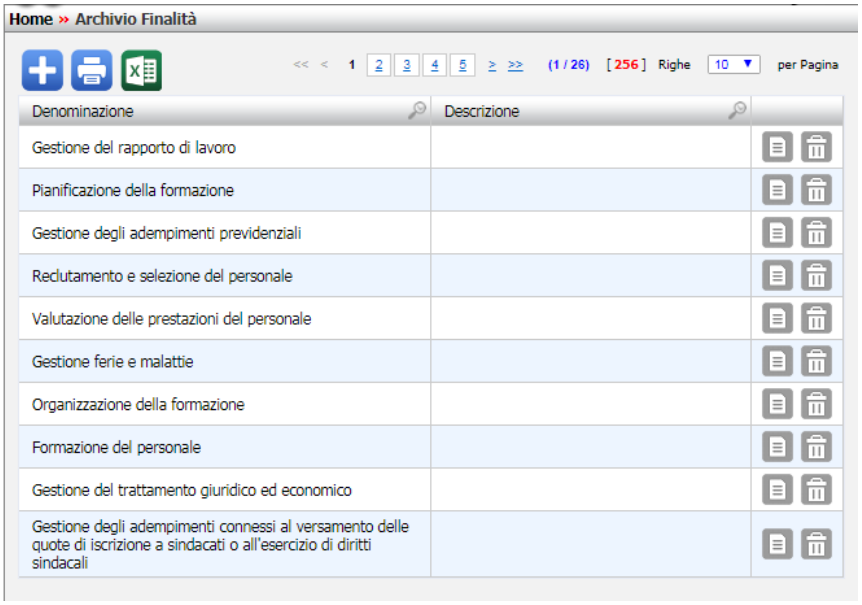
Il modulo è strutturato in due sezioni: una barra dei menu, all'interno della quale sono presenti le seguenti voci: HOME, ARCHIVI, ANAGRAFICA, STAMPE, DPIA ed ESCI,

e quello che è il cuore del modulo all'interno della sezione Home, cioè l'intero flusso dei dati per la gestione della privacy.

2.1 ARCHIVI

All'interno del modulo sono presenti degli archivi di base già pre-compilati, ma ulteriormente ampliabili dall'utente. Questi archivi aiutano nella compilazione del flusso della privacy, permettendo di individuare le voci di interesse ed importarle all'interno del flusso stesso.





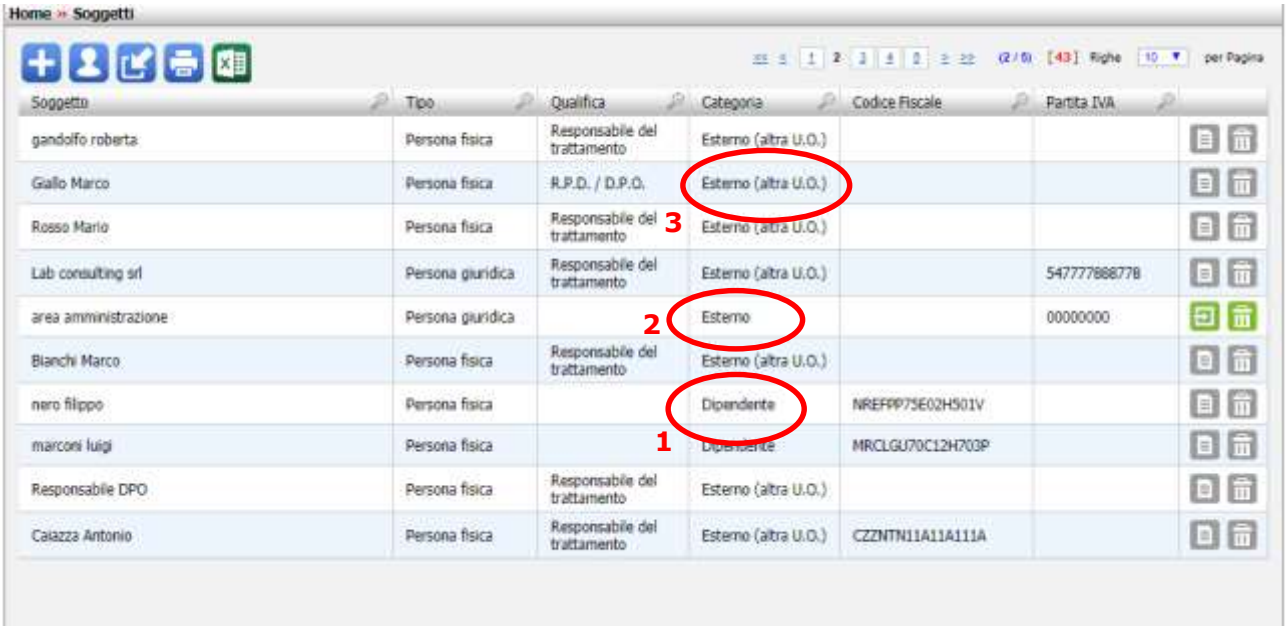
È possibile, inoltre, aggiungere, in qualsiasi momento, delle nuove voci all'interno di ogni archivio attraverso il tasto più. Le voci così aggiunte saranno sempre disponibili all'interno degli archivi stessi.

2.2 ANAGRAFICA

Dalla sezione anagrafica, sarà possibile richiamare i soggetti all'interno del flusso della privacy ogni qual volta si dovrà inserire un nominativo.
Tale anagrafica si compone di:

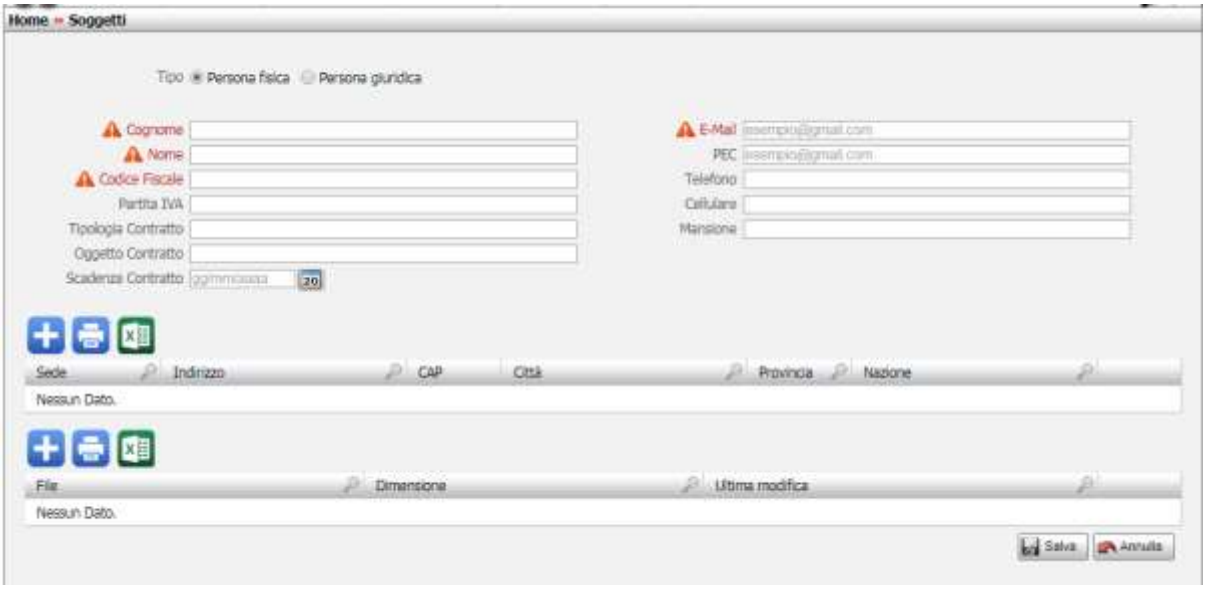
- soggetti **interni** all'azienda. Tali soggetti vengono inseriti all'interno del back office nella sezione delle risorse umane, come illustrato al punto 1.4; tutte le risorse, inserite nel back office, saranno, quindi, riconosciute dal sistema come soggetti interni e nella colonna Categorie, presente all'interno della sezione, saranno indicati con la dicitura "Dipendenti" (1).
- soggetti **esterni** (es. consulenti, commercialisti o altro personale esterno all'azienda che saranno i possibili responsabili del trattamento o DPO). Tali soggetti vanno inseriti, direttamente, all'interno di tale sezione di anagrafica nel modulo privacy. Solo così il sistema li riconoscerà come soggetti esterni e li inserirà con la dicitura "Esterno" (2).
- soggetti **esterni (altra U. O.)**: all'interno dell'anagrafica, vengono richiamati anche eventuali Responsabili del trattamento e DPO nominati in altre unità organizzative

inserite all'interno del sistema; anche in questo caso il sistema li riconoscerà come soggetti esterni e li inserirà con la dicitura "Esterno (altra U.O.)" (3).



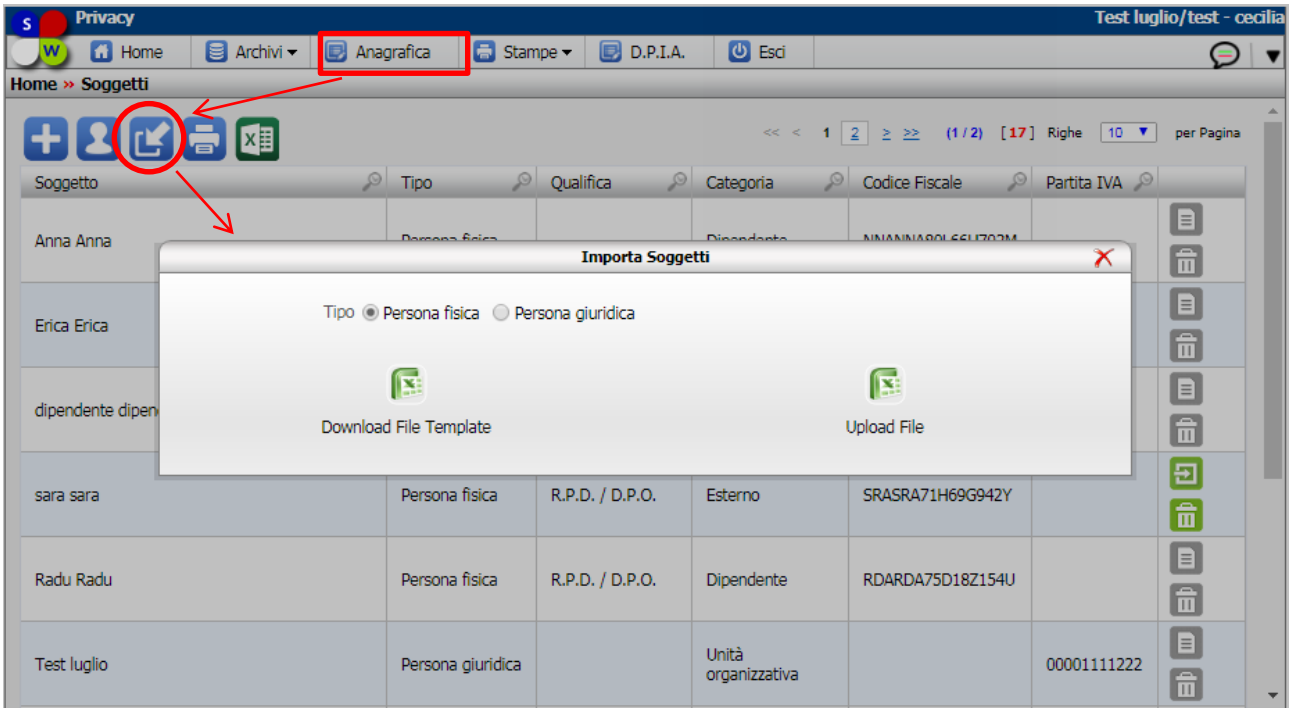
N.B. La distinzione tra soggetti interni e soggetti esterni è un punto importante in quanto sui soggetti esterni il sistema permette di fare la stampa della nomina del responsabile del trattamento secondo l'art. 28 del nuovo Regolamento Europeo *UE 2016/679*; tale stampa sarà disponibile solo in caso di soggetti che il sistema individua come esterni o esterni (altra U.O.).

Per creare l'anagrafica di un soggetto esterno, selezionare il comando "Nuovo Soggetto" : si aprirà il form seguente:



Sarà necessario compilare i vari campi e fare salva per salvare il soggetto all'interno dell'anagrafica. I campi obbligatori sono quelli in rosso, ma va precisato che i due campi, "Tipologia di contratto" e "Oggetto contratto", vengono richiamati all'interno della stampa della nomina del responsabile del trattamento.

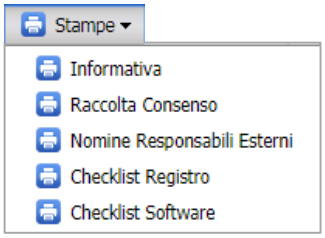
In alternativa si può procedere attraverso un caricamento massivo di più soggetti esterni da file Excel (download/upload template per persona fisica e per persona giuridica).
Si dovrà procedere prima a scaricare il template scegliendo il Tipo di soggetti da inserire persone fisiche o persone giuridiche; compilare il template con i dati da inserire e proceder quindi all'upload del file generato.



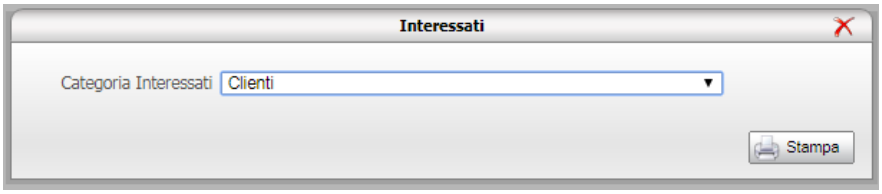
2.3 STAMPE

Selezionando la voce Stampe, posta in alto all'interno della barra dei menu, sarà visualizzata la sezione per comporre le seguenti stampe:

- **Informativa**
- **Raccolta consenso**
- **Nomine Responsabili Esterni**
- **Checklist Registro**
- **Checklist Software**



Per effettuare la stampa dell'informativa e della raccolta consenso si dovrà selezionare la categoria di interessati per cui si vuole effettuare la stampa.



Cliccando su **Nomine Responsabili Esterni** si aprirà la seguente finestra di dialogo:

dalla quale sarà possibile selezionare i responsabili per cui si vuole stampare la nomina, inserire la data di inizio e la data di fine del contratto/servizio principale che verrà riportata sulla stampa stessa, e cliccare sul comando "**stampa**"; il sistema genera un file .zip in cui saranno raggruppate tutte le nomine dei responsabili selezionati.

Le ultime due stampe permetto di generare delle check list, che aiutano nella fase di analisi iniziale, per individuare le informazioni che si dovranno inserire all'interno del sistema (checklist software) ed una check list di verifica avente ad oggetto il REGISTRO dei TRATTAMENTI del TITOLARE (checklist registro).

2.4 HOME

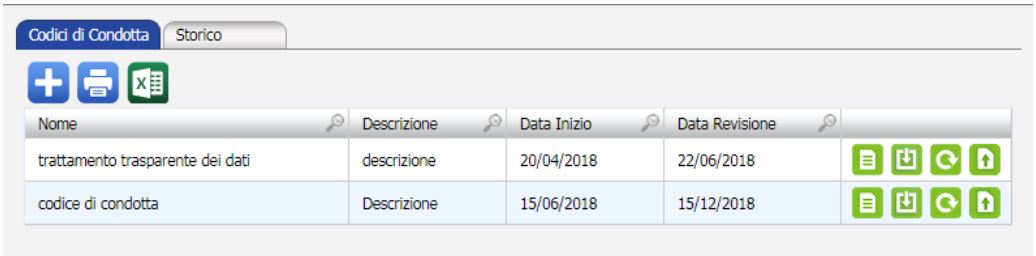
Dalla voce Home si può accedere alle sezioni dell'intero flusso della privacy:

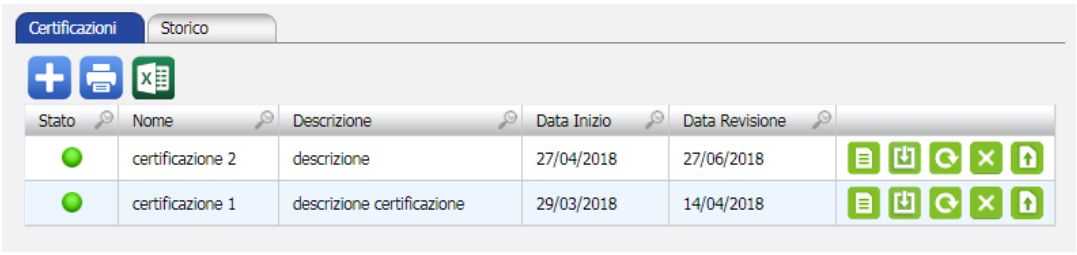
- **Codici e Certificazioni**
- **Trattamenti**
- **Conservazione Dati**
- **Soggetti Autorizzati**
- **Asset**
- **Registro Trattamenti**

Per poter accedere e lavorare su ognuna di tali sezioni, basterà selezionarle ed aprirle: si aprirà, così, la singola sezione di composizione, dalla quale sarà possibile procedere alla compilazione della stessa, come meglio spiegato di seguito.

2.4.1. CODICI E CERTIFICAZIONI

Per accedere a questa sezione basta selezionare dalla Home la voce corrispondente. All'interno di questa sezione è possibile inserire eventuali codici di condotta e certificazione che l'azienda ha deciso di adottare.





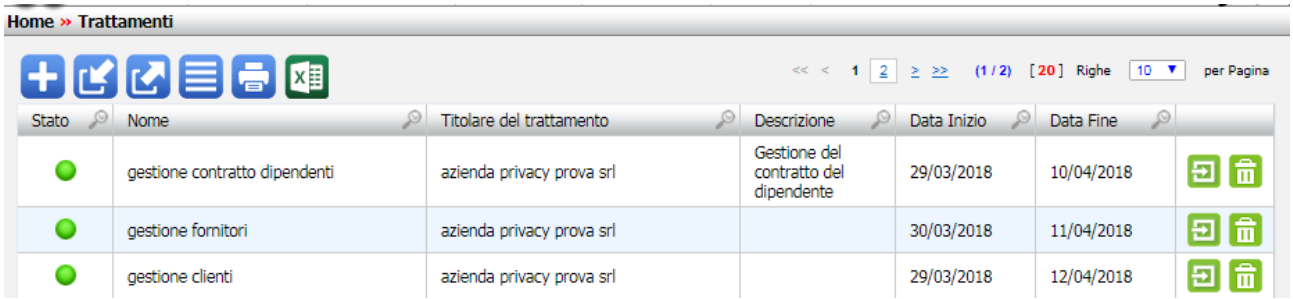
Attraverso il tasto sarà possibile inserire un codice di condotta o una certificazione dell'azienda compilando l'apposito form contenete il nome, la descrizione, la data di inizio e la data di revisione.

A destra di ogni riga sono presenti, in ordine, i seguenti comandi:

- **dettagli**: tale comando permette di accedere al form di compilazione del codice di condotta o certificazione per modificarlo;
- **storicizza**: permette di storicizzare il codice di condotta o la certificazione spostandoli nella scheda storico;
- **rinnova**: permette di rinnovare il codice di condotta o la certificazione creandone una copia e spostando la vecchia nello storico;
- **revoca**: modifica lo stato della certificazione da attivo a revocato;
- **allegati**: permette di allegare dei file, relativamente ai codici di condotta o alle certificazioni, all'interno del sistema.

2.4.2. TRATTAMENTI

Attraverso questa sezione è possibile creare e, quindi, gestire i trattamenti relativi ai dati personali.
Per accedere a questa sezione basta selezionare all'interno della Home la voce corrispondente.
Si apre così la seguente schermata, dalla quale è possibile lavorare sui trattamenti.



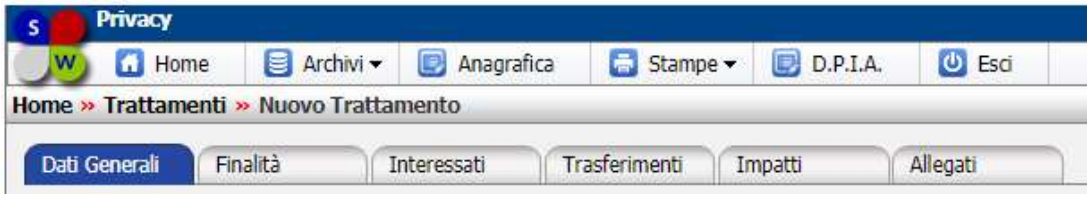
Nella parte superiore della finestra, sotto la voce Home>>Trattamenti, sono presenti, in ordine, i seguenti comandi:

- **Nuovo trattamento**: tale comando permette di creare un nuovo trattamento;
- **Importa Trattamenti**: permette di importare, sotto forma di un file ".xml", all'interno di un'unità organizzativa un singolo trattamento o un insieme di trattamenti creati in un'altra unità organizzativa;
- **Esporta Trattamenti**: permette di esportare un trattamento o un insieme di trattamenti, creati in un'unità organizzativa, salvando un file ".xml" che potrà poi essere importato all'interno di un'altra unità organizzativa;
- **Mostra revocati**: visualizza i trattamenti revocati;

- **Stampa**: permette di stampare i dati riportati a video.
- **Stampa tabella**: permette di estrapolare, in un file excel, i dati riportati a video.

2.4.2.1. CREAZIONE DI UN NUOVO TRATTAMENTO

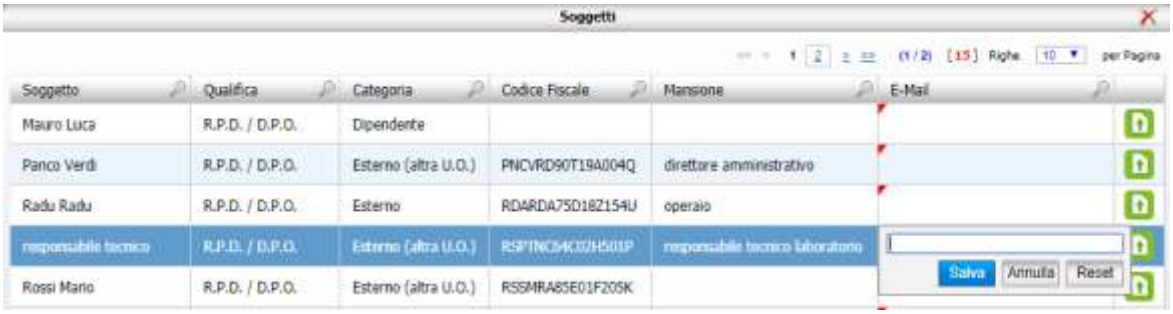
Per creare un **nuovo trattamento** selezionare il comando "Nuovo Trattamento", si aprirà una schermata suddivisa in cinque schede: Dati Generali, Finalità, Interessati, Trasferimenti, Allegati.



1. Dalla prima scheda "**DATI GENERALI**" è necessario inserire il **nome del trattamento** e le figure responsabili legate a tale trattamento: in modo particolare, **Titolare del Trattamento**, e se nominati, Responsabile del trattamento ed R.P.D./D.P.O.. Per inserire tali figure è sufficiente cliccare sul tasto "modifica": si aprirà la sezione di anagrafica dalla quale è possibile individuare il soggetto per ogni particolare figura da inserire ed importarlo.

   In particolare, quando viene creato un nuovo trattamento, il software riporta in automatico, nel campo Titolare del Trattamento, la società, intesa come persona giuridica, così come creata nell'anagrafica dell'unità organizzativa all'interno del back office.

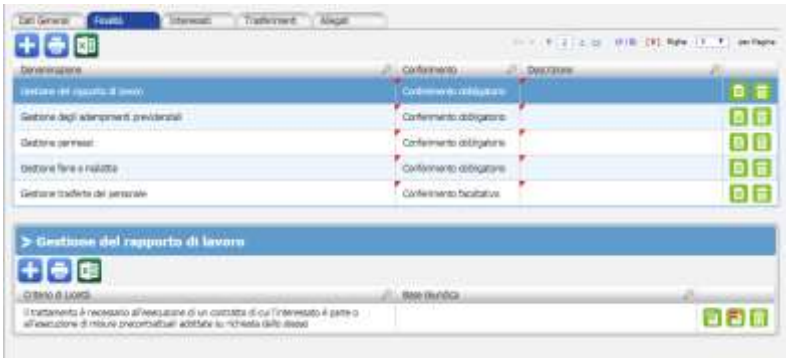
   Inoltre, nel campo R.P.D./D.P.O. e nel campo Responsabile del Trattamento quando si importano i nominativi dall'anagrafica, è possibile modificare la mail; ciò permetterà di individuare in modo univoco per singolo ente/azienda i riferimenti di contatto di un DPO condiviso.



   Va poi indicata la **data di inizio** e **di verifica** del trattamento inserito. Nell'ultima sezione della scheda, va indicato se i dati vengo profilati ed eventualmente trattati con **processi automatizzati**, e, in tal caso, inserire una descrizione di tali processi.

2. Completata la scheda dei Dati Generali, spostarsi nella scheda "**FINALITÀ"**. All'interno di tale scheda individuare le **finalità** del trattamento appena creato, ciò al fine di rendere leggittimo tale trattamento. Per inserire tali finalità, selezionare l'apposito comando : si aprirà un archivio "FINALITÀ", dal quale è possibile richiamare le finalità d'interesse. Le voci presenti non sono modificabili, ma è possibile inserirne delle nuove (come spiegato al punto 2.1). Per ogni finalità, attraverso il comando situato a destra è possibile inserire i criteri di liceità (richiamabile sempre da archivi precaricati)

e le relative basi di giuridiche e scegliere se il conferimento dei dati, per ogni finalità, è obbligatorio o facoltativo.



3. Completata la scheda Finalità, spostarsi nella scheda "**INTERESSATI".** All'interno di tale scheda individuare gli **interessati** al trattamento attraverso il comando : si aprirà un archivio "CATEGORIE INTERESSATI", dal quale è possibile richiamare le la categoria di interessati.

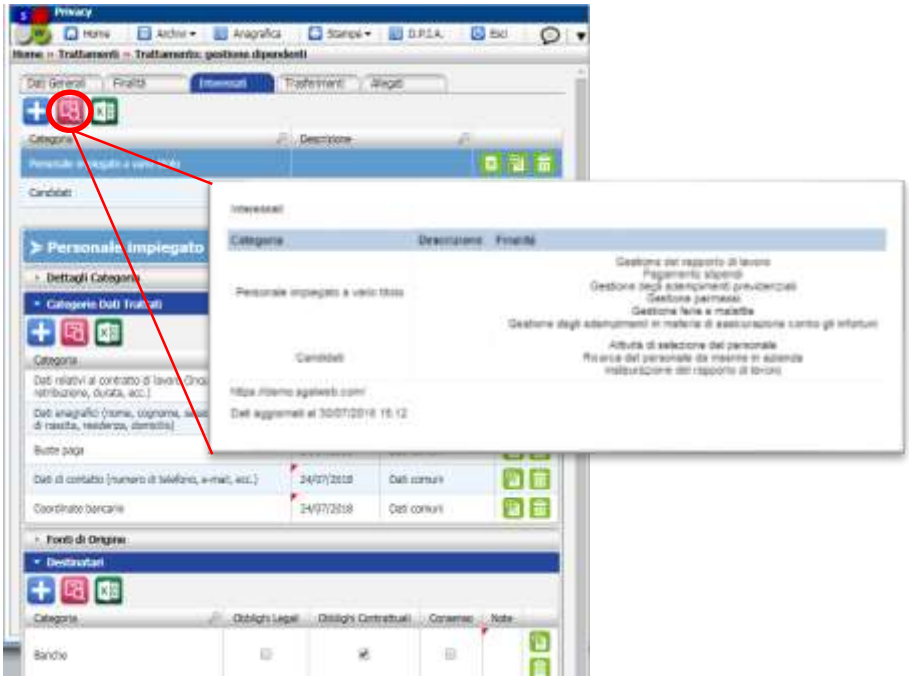
   Nella creazione del trattamento, un passo cruciale è l'assegnazione di ogni finalità ad una categoria di interessati inserita, a cui il trattamento dei dati si riferisce. All'interno di un trattamento si possono individuare più categorie di interessati, ma non per tutti si ottengono le stesse finalità. È necessario, quindi, associare le finalità ad ogni categoria di interessati inserita.

   Per fare ciò, dalla finestra che si apre, cliccando sull'apposito comando "finalità" mettere il segno di spunta sulle finalità collegate alla singola categoria di interessati e salvare la schermata.

Per maggiori dettagli **visitare la seguente pagina web:**

https://www.sgslweb.it/2018/05/18/trattamento-associazioni-interessati-e-finalita-privacy-gdpr/

Sarà possibile, in ogni momento, attraverso il tasto visualizzare i dettagli delle associazioni fatte tra interessati e finalità, dati trattati e finalità, e destinatari e finalità.



Per ogni categoria di interessati, vanno poi compilate le sezioni sottostanti che si aprono cliccando sul comando dettagli posizionato a destra di ogni riga.

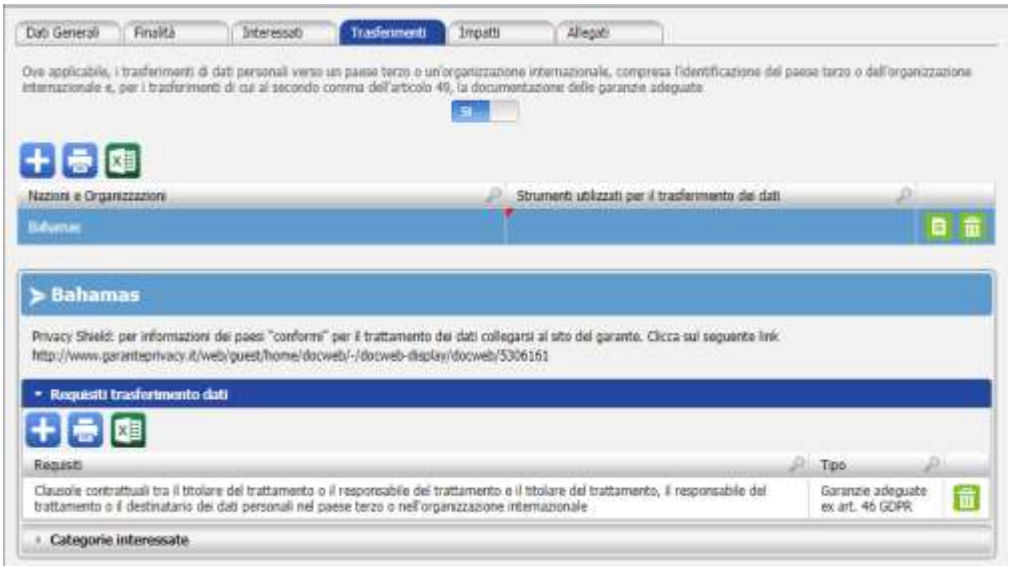
In modo particolare, specificare quali dati personali (**categoria dati trattati**) sta trattando il titolare e per quali finalità; per fare ciò è sufficiente selezionare il tasto "importa" e dall'archivio corrispondente che si apre, importare le voci di interesse. Per ogni dato trattato, vanno poi specificate per quali finalità vengono trattati selezionandole dalla finestra di dialogo che si apre cliccando sul tasto "finalità", posto a destra di ogni riga.

È necessario, quindi, indicare quali sono le **fonti di origine** dei dati trattati importandole dall'archivio corrispondente che si apre attraverso il comando "importa".

Specificare i **destinatari** a cui i dati trattati sono o saranno comunicati, sempre importandoli dal corrisppondente archivio che si apre attraverso il comando "importa"; per ognuno di essi va, poi, indicato se si tratta di obblighi legali, contrattuali o se è necessario richiedere il consenso agli intererssati. Infine, va specificato per quali finalità vengono comunicati i dati a tali destinatari, selezionando le stesse dalla finestra di dialogo che si apre cliccando sul tasto "finalità", posto a destra di ogni riga.

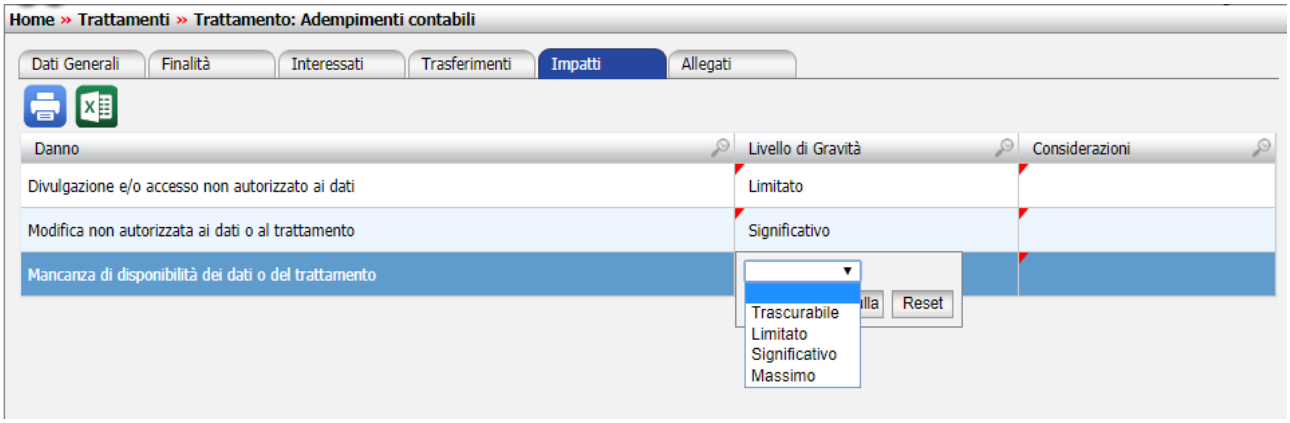
Nelle ultime due sezione "**categorie particolari di dati personali**" e "**dati personali relativi a condanne o reati**" si può inserire, nel caso in cui si stanno trattando categorie particolari di dati ex art.9 o ex art.10 (dati sensibili), qual è la condizione del trattamento; anche in questo caso, è possibile importare tale criterio dall'archivio corrispondente.

4. Completata la scheda Interessati, spostarsi nella scheda "**TRASFERIMENTI".** in tale scheda, è possibile indicare eventuali destinatari di paesi terzi od organizzazioni internazionali verso cui avviene il trasferimento di dati personali di una categoria di interessati ed i relativi requisiti per tale trasferimento, secondo quanto specificato dall'articolo 49 del nuovo Regolamento Europeo sulla Protezione dei Dati (UE 2016/679).
   Per fare ciò, spostare il flag sul **SI** e dalla sezione sottostante che si apre inserire i dati importandoli dagli archivi corrispondenti che si visualizzano attraverso l'apposito comando "importa".



5. Nella scheda "**IMPATTI"** si tiene conto di quelli che sono i rischi che il trattamento comporta sulla protezione dei dati e dell'impatto che una possibile perdita di sicurezza dei dati può avere sui diritti e sulle libertà fondamentali delle persone fisiche interessate:

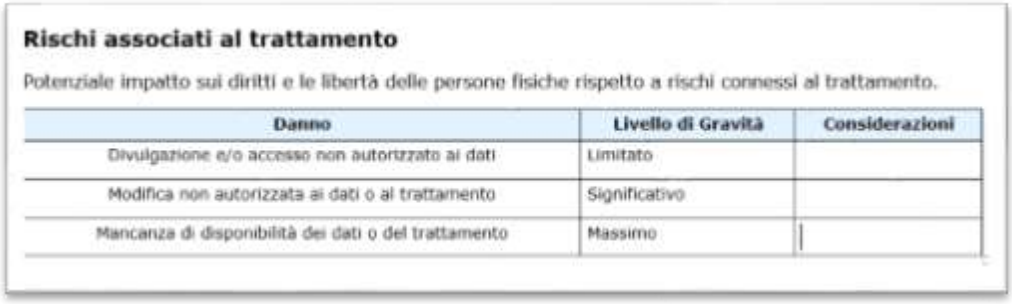
- Divulgazione e/o accesso non autorizzato ai dati
- Modifica non autorizzata ai dati o al trattamento
- Mancanza di disponibilità dei dati o del trattamento



Ad ogni danno va associato il rispettivo livello di gravità valutato su quattro possibili valori:

- Trascurabile
- Limitato
- Significativo
- Massimo

Tali informazioni sono quindi riportate all'interno della stampa del registro del trattamento, dove comparirà una sezione Rischi associati al trattamento come mostrato in figura:

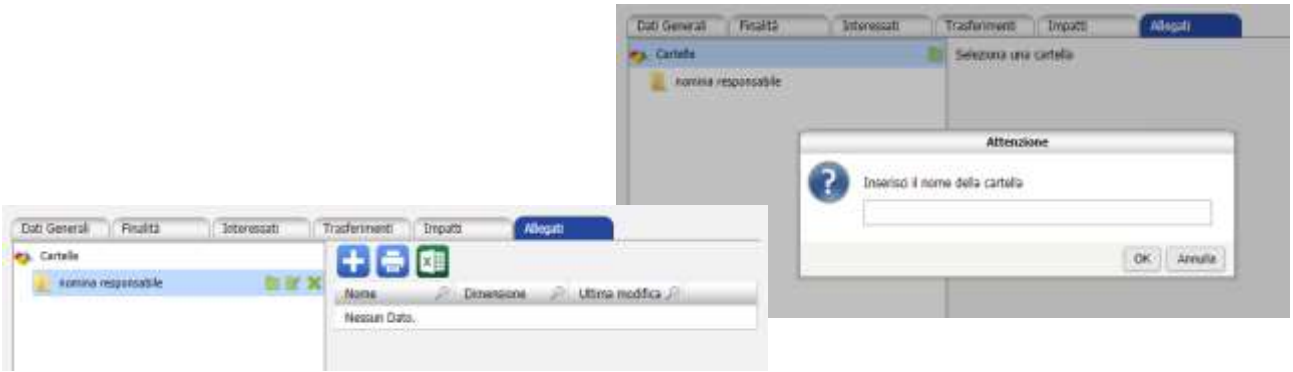


Rischi associati al trattamento

Potenziale impatto sui diritti e le libertà delle persone fisiche rispetto a rischi connessi al trattamento.

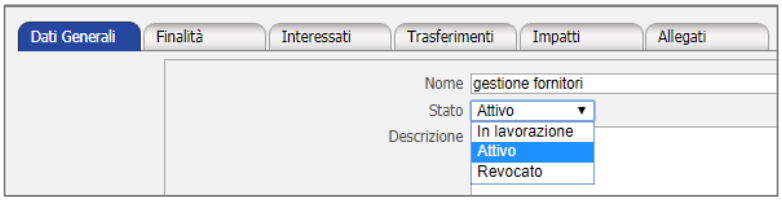
Danno	Livello di Gravità	Considerazioni
Divulgazione e/o accesso non autorizzato ai dati	Limitato	
Modifica non autorizzata ai dati o al trattamento	Significativo	
Mancanza di disponibilità dei dati o del trattamento	Massimo	

6. Nella scheda "**ALLEGATI"** sarà possibile inserire cartelle e sottocartelle e caricare dei file all'interno del sistema.



IMPORTANTE: ogni trattamento ha tre possibili stati che si possono impostare nella sezione dei Trattamenti dalla scheda dei Dati Generali all'interno della voce stato:

- **Attivo,**
- **In Lavorazione,**
- **Revocato**

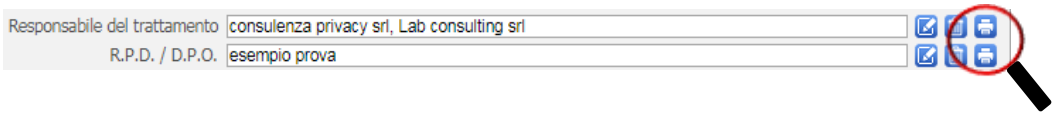


All'interno delle stampe compaiono solo i trattamenti in stato attivo; durante la fase di creazione di un trattamento lo stato dello stesso è posto "in lavorazione", per visualizzarlo all'interno delle stampe, sarà, quindi, necessario modificarne lo stato.

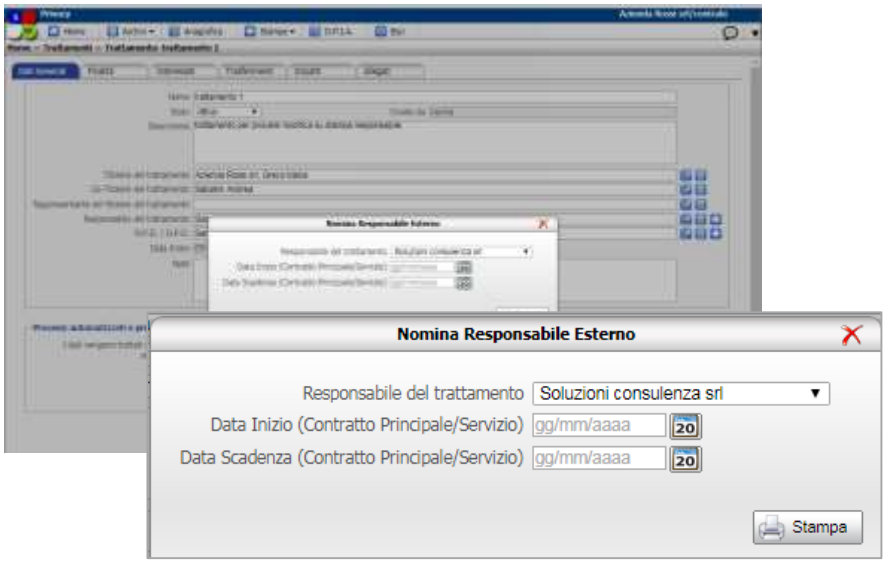
È sempre possibile in ogni momento cambiare lo stato ad un trattamento.

2.4.2.2. STAMPA CONTRATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO O DPO/RPD

Dalla sezione Trattamenti nella scheda Dati Generali sarà possibile procedere alla stampa della ***Nomina del Responsabile del Trattamento***, quando è un soggetto esterno, e alla stampa dell'***Atto di designazione del DPO/RPD***, utilizzando l'apposito tasto posizionato a destra delle rispettive righe.

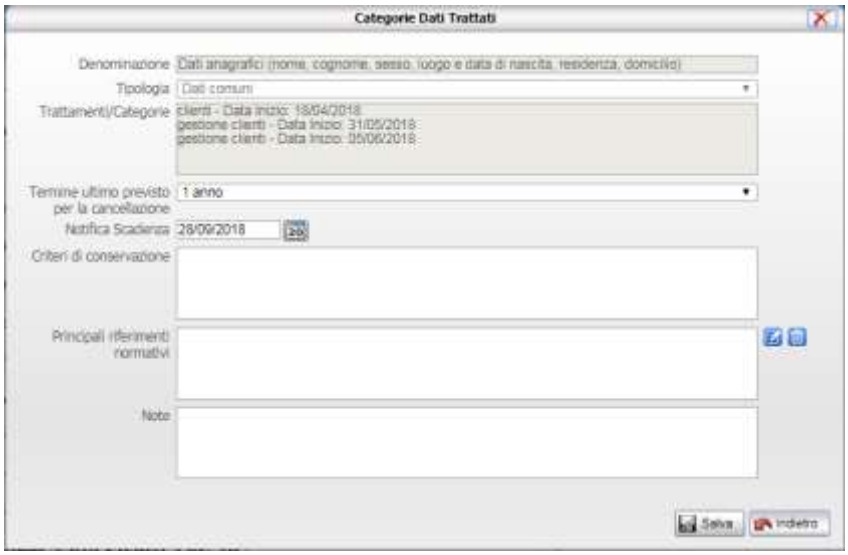


Nella stampa della nomina del Responsabile del trattamento, è possibile inserire la data di stipula e la data di scadenza del contratto principale/servizio direttamente da software prima di procedere alla stampa stessa; tali date, se inserite, vengono riportate sulla stampa della nomina, altrimenti, nella stampa compariranno campi vuoti.



2.4.3. CONSERVAZIONE DEI DATI

Per accedere a questa sezione basta selezionare, dalla Home, la voce corrispondente.
All'interno di questa sezione, per ogni categoria di interessati, saranno riportati i dati trattati e il numero di trattamenti collegati ad essi. Aprendo i dettagli, attraverso l'apposito comando, posizionato a destra di ogni riga, è possibile inserire la **durata di conservazione** e i termini ultimi previsti per la cancellazione degli stessi e specificare eventuali criteri di conservazione e riferimenti normativi.



2.4.4. SOGGETTI AUTORIZZATI

Per accedere a questa sezione, basta selezionare, dalla Home, la voce corrispondente.

All'interno di questa sezione, sarà possibile individuare i **soggetti autorizzati** per ogni trattamento, ad accedere ai dati trattati e le relative modalità di accesso (es.: consultazione, raccolta, conservazione, etc.). È possibile autorizzare anche più soggetti contemporaneamente.

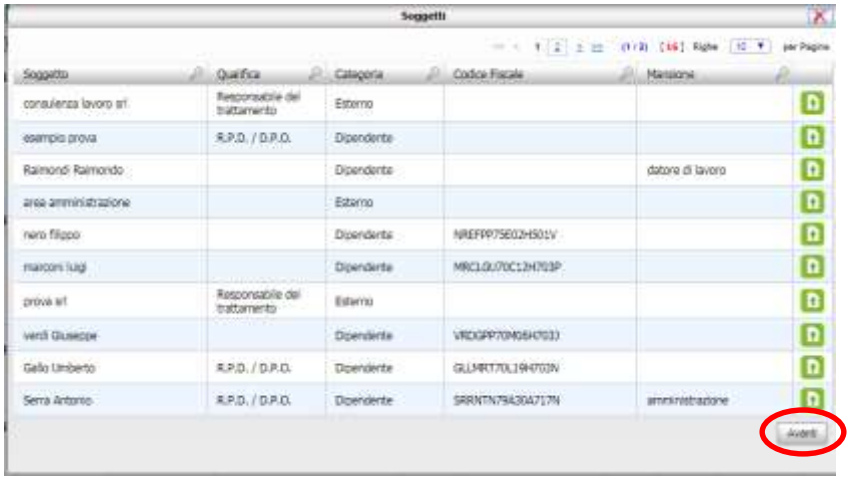
Per fare ciò, selezionare il tasto "nuovo" , si aprirà una finestra di dialogo che attraverso tre passi successivi permette di:

PASSO 1. Individuare ed importare il singolo soggetto, o anche più soggetti insieme, da autorizzare e premere il tasto "avanti";

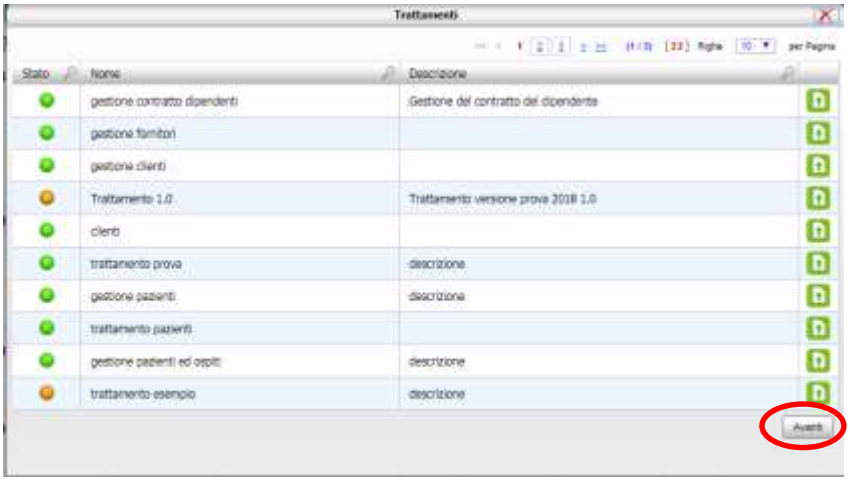
PASSO 2. Individuare ed importare i trattamenti per cui si sta autorizzando i soggetti e premere il tasto "avanti";

PASSO 3. Individuare ed assegnare i permessi con cui trattare i dati ai soggetti e premere il tasto "salva";

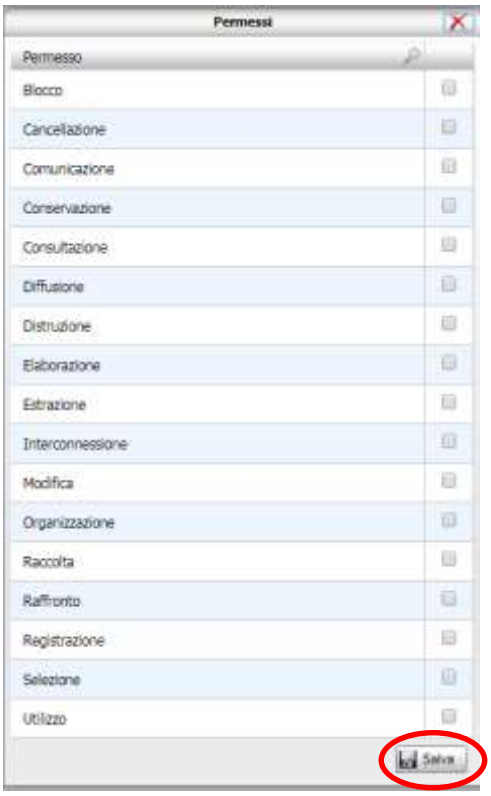
Passo 1



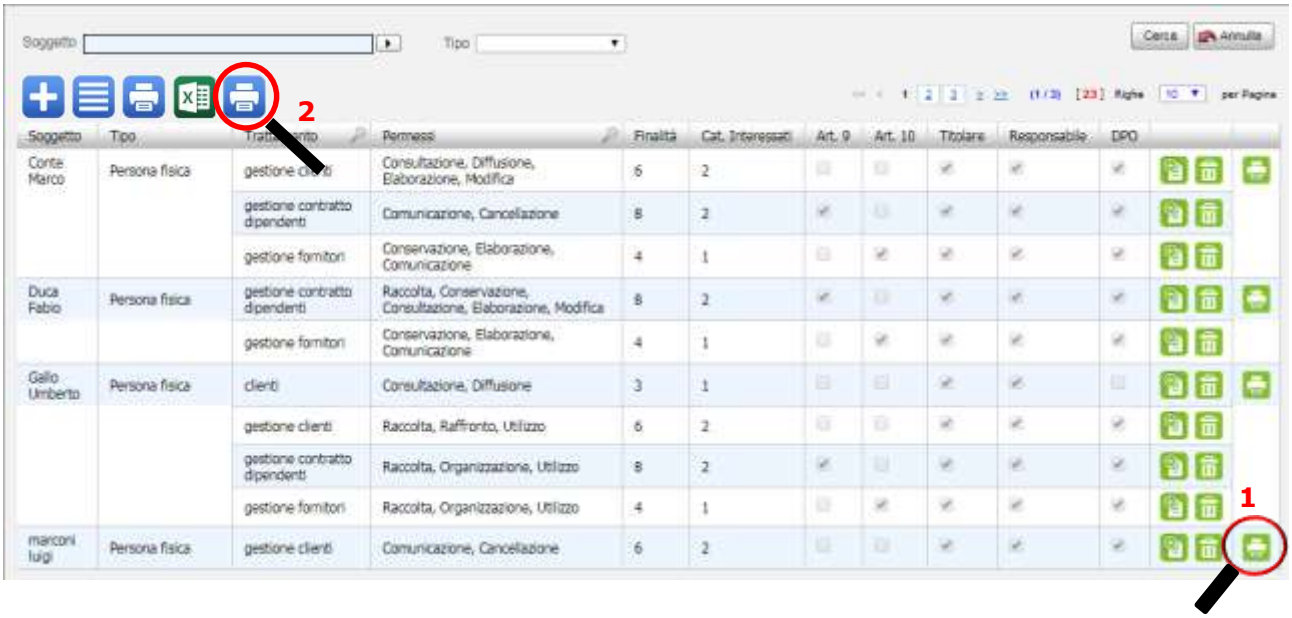
Passo 2



Passo 3



Durante la fase di creazione passo – passo non si visualizzerà niente, solo con il salvataggio al passo 3 il sistema visualizzerà, all'interno della schermata principale, i soggetti autorizzati.

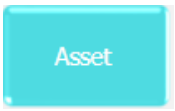


Individuati i soggetti autorizzati, per ognuno di loro, è possibile ***stampare la lettera di incarico*** attraverso l'apposito tasto di stampa (1).

In alternativa si può procedere ad una stampa massiva di tutte le lettere di incarico dei soggetti autorizzati attraverso un unico file .zip (2).

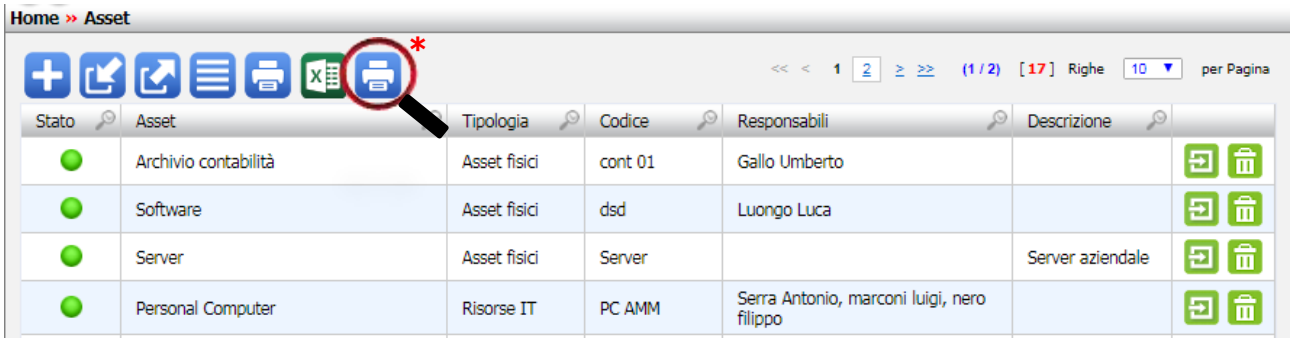
2.4.5. ASSET

Tale sezione permette di individuare e creare gli **asset**, cioè tutti quei beni materiali e non, che creano produttività all'azienda e su cui ho collegati dei dati personali.
Per accedere a tale sezione selezionare, dalla Home, la voce corrispondente.



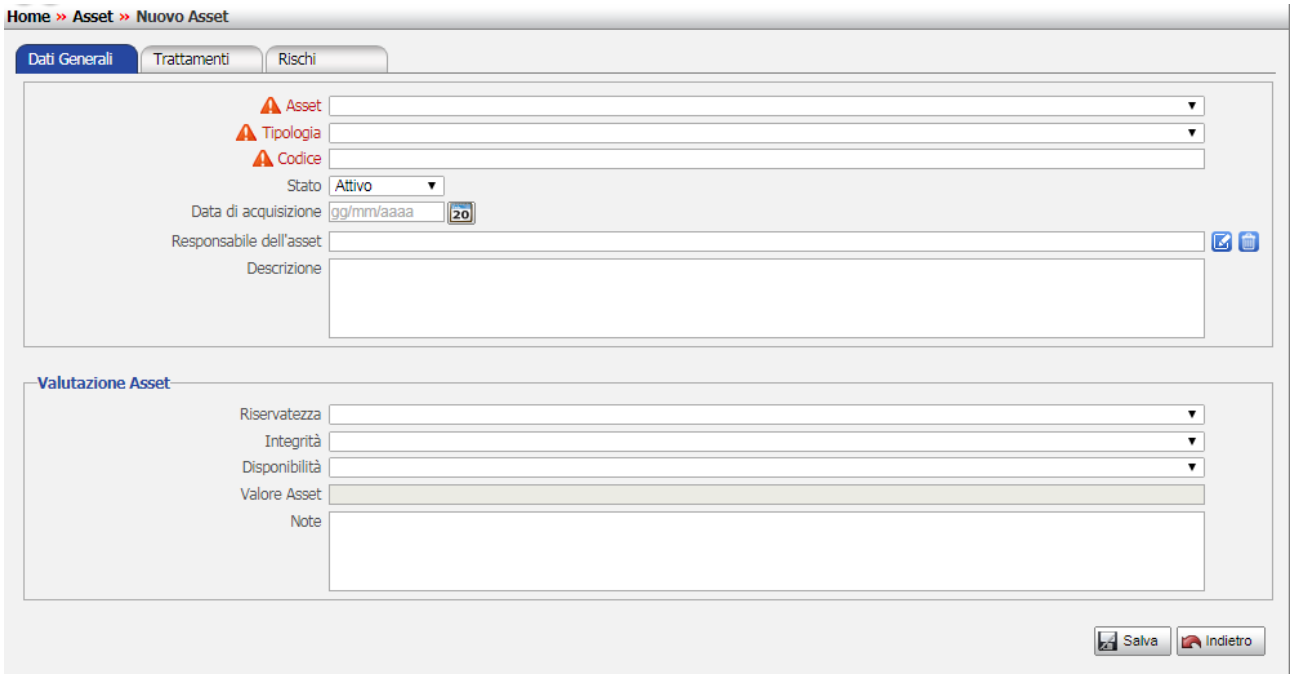
Si aprirà una schermata dalla quale sarà possibile creare e lavorare sugli asset.
Nella parte superiore della finestra, sotto la voce Home>>Asset, sono presenti, in ordine, i seguenti comandi:

- **Nuovo Asset**: tale comando permette di creare un nuovo asset;
- **Importa Asset**: permette di importare, sotto forma di un file ".xml", all'interno di un'unità organizzativa un singolo asset o un insieme di asset creati in un'altra unità organizzativa;
- **Esporta Asset**: permette di esportare un asset o un insieme di asset, creati in un'unità organizzativa, salvando un file ".xml" che potrà poi essere importato all'interno di un'altra unità organizzativa;
- **Mostra revocati**: visualizza gli asset revocati;
- **Stampa**: permette di stampare i dati riportati a video;
- **Stampa tabella**: permette di estrapolare, in un file excel, i dati riportati a video;
- **Stampa dettagli***: permette di stampare uno o più asset selezionati; tale stampa riporta tutte le informazione inserite nel sistema e relative ai singoli asset stampati.



2.4.5.1. CREAZIONE DI UN NUOVO ASSET

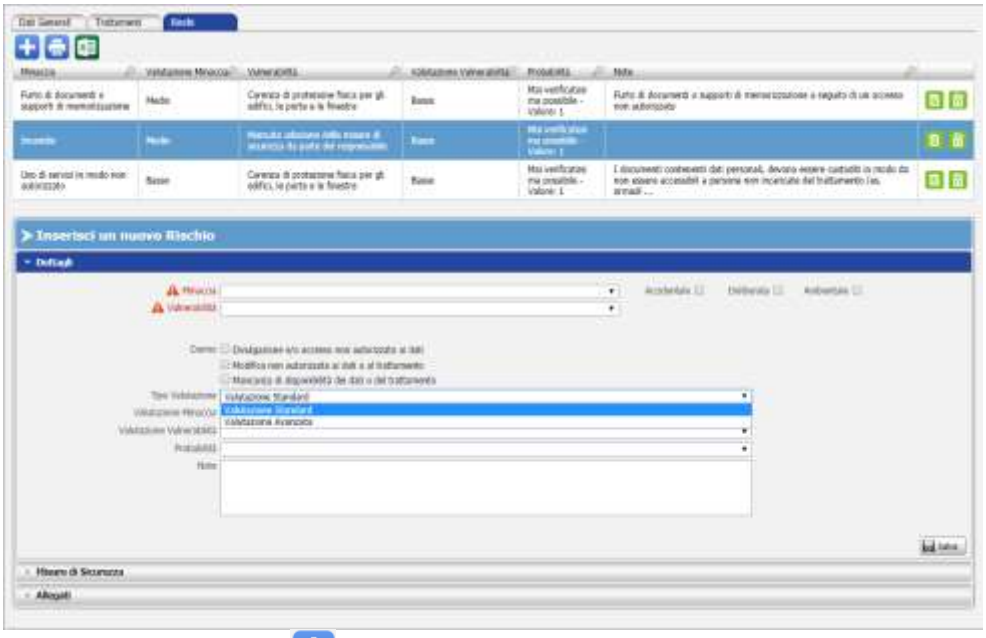
Per creare un **nuovo asset** selezionare il comando "Nuovo Asset"; si aprirà una schermata suddivisa in tre schede: Dati Generali, Trattamenti, Rischi.



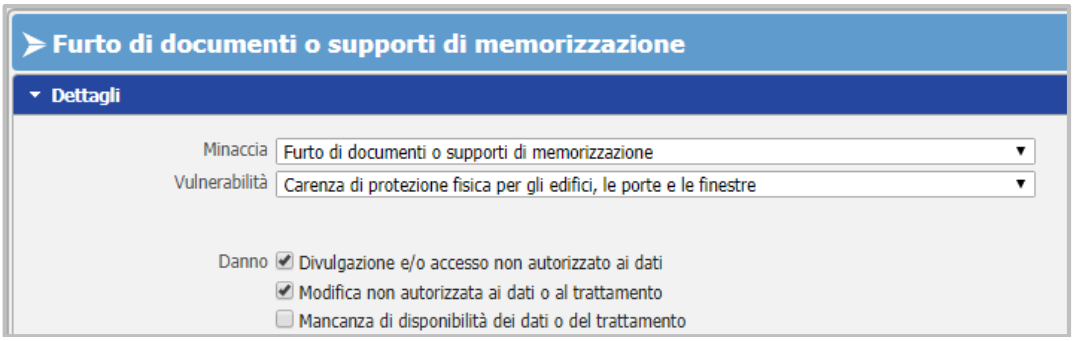
Dalla prima scheda "**DATI GENERALI**" è necessario inserire l'**asset** e la **tipologia**, richiamandoli dagli archivi corrispondenti che si aprono nelle rispettive sezioni, assegnare quindi un **codice** all'asset, la **data di acquisizione** ed il **responsabile** di tale asset.
Si passa, quindi, a valutare la sicurezza dell'asset in base alla **riservatezza**, all'**integrità** e alla **disponibilità**.

Dalla seconda scheda "**TRATTAMENTI**" è possibile importare, dalla finestra di dialogo che si apre utilizzando il tasto "nuovo" , i trattamenti legati all'asset.

Nell'ultima scheda "**RISCHI**" vanno individuate le possibili minacce e le relative misure di sicurezza tecniche e/o organizzative adottate o da adottare per prevenirle.



A tale scopo, attraverso il tasto , si apre la sezione "inserisci un nuovo Rischio" dalla quale è possibile individuare, importandola dall'archivio corrispondente, la **minaccia** legata all'asset in esame. Per ogni minaccia, si dovrà vedere se l'evento è di tipo "Accidentale", "Deliberata" o "Ambientale" e si dovrà, quindi, individuare una possibile **vulnerabilità** legata a tale minaccia. Sarà possibile indicare, inoltre, su cosa impatta la minaccia, mettendo la spunta sul rispettivo danno: perdita di riservatezza, perdita di integrità, perdita di disponibilità.



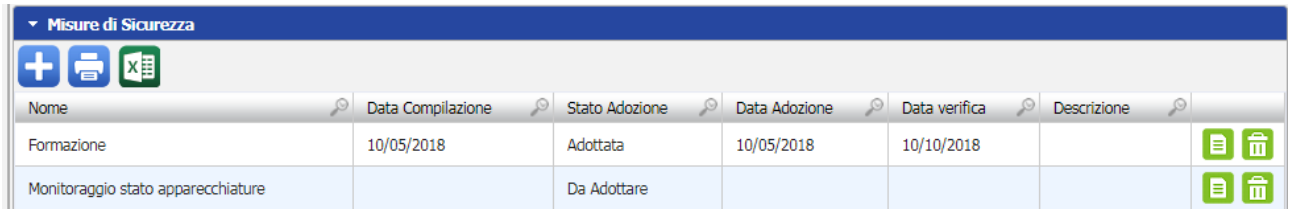
A questo punto si sceglie il tipo di valutazione del rischio che si vuole effettuare: **valutazione standard** o **valutazione avanzata** ed in base alla scelta fatta si procede con l'individuazione della probabilità del rischio in funzione della vulnerabilità e della minaccia.

Per maggiori dettagli sulla metodologia della valutazione del rischio **visitare le seguenti pagine web:**

valutazione standard del rischio:
www.sgslweb.it/2018/06/25/risk-assesment-metodologia-analisi-dei-rischi-sulla-protezione-dei-dati-personali/

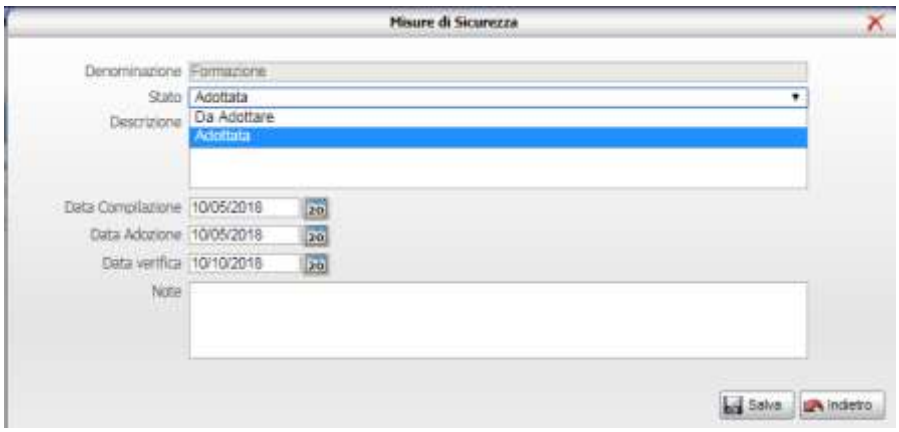
valutazione avanzata del rischio:
www.sgslweb.it/2019/01/07/privacy-valutazione-avanzata-del-rischio/

Dopo aver fatto una valutazione della minaccia, della vulnerabilità e della probabilità che tale minaccia si verifichi, si procede ad individuare le **misure di sicurezza** che si vogliono adottare o che, eventualmente, si sono già adottate per ridurre tale minaccia.

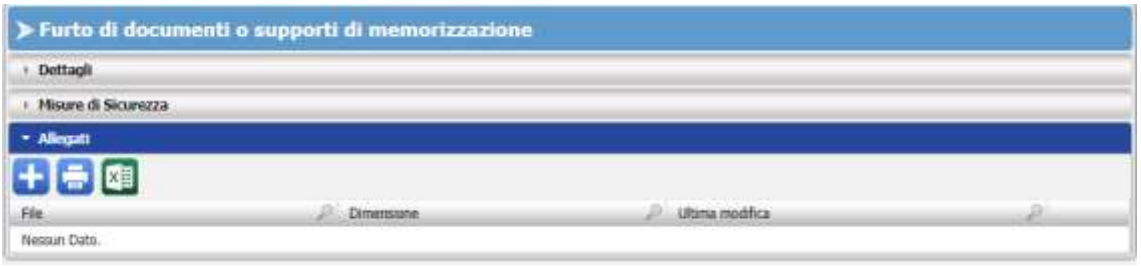


Per individuare le misure di sicurezza, è possibile importarle da un archivio che si apre cliccando sul tasto .

Inserite le misure di sicurezza, attraverso il tasto "**dettagli**" posta a destra di ogni riga, sarà possibile indicare lo stato della stessa se adottata o da adottare ed inserire la data di compilazione, la data di adozione (o data prevista se la misura di sicurezza non è stata ancora adottata) e la data di verifica.

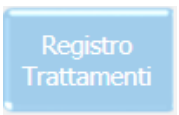


Nella sezione sottostante le misure di sicurezza, sarà invece possibile allegare dei file all'interno di ogni minaccia.



2.4.6. REGISTRO TRATTAMENTI

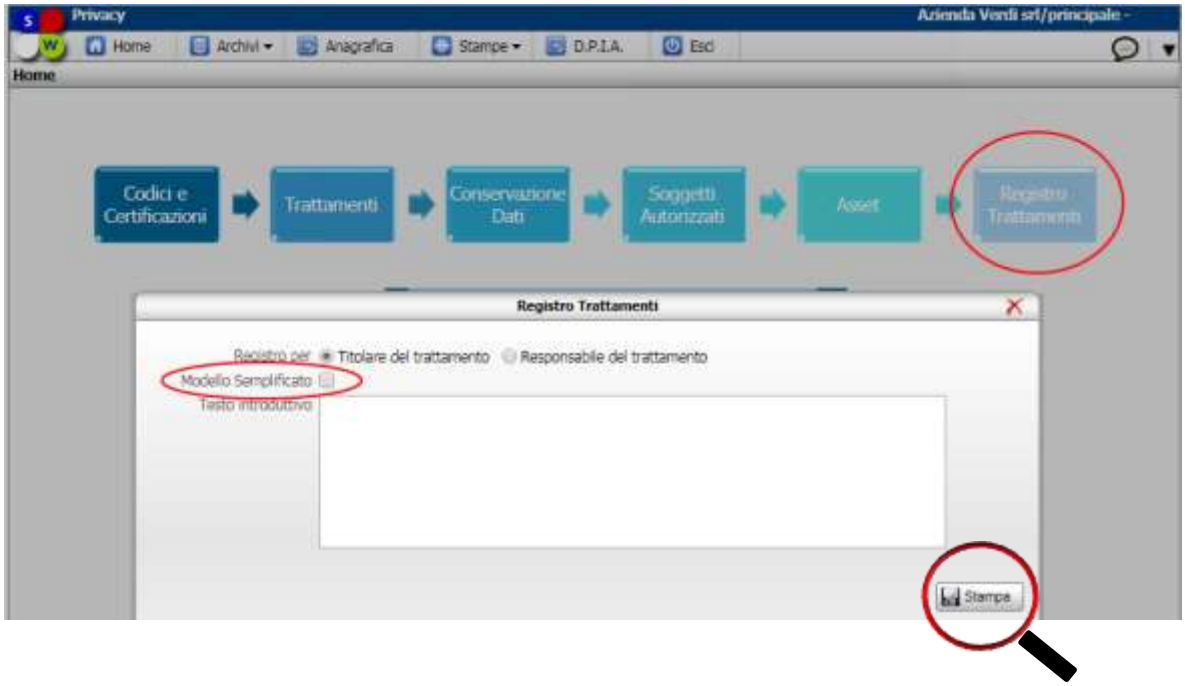
Tale sezione permette la tenuta del registro dei trattamenti, come previsto dall'art. 30 del regolamento europeo.



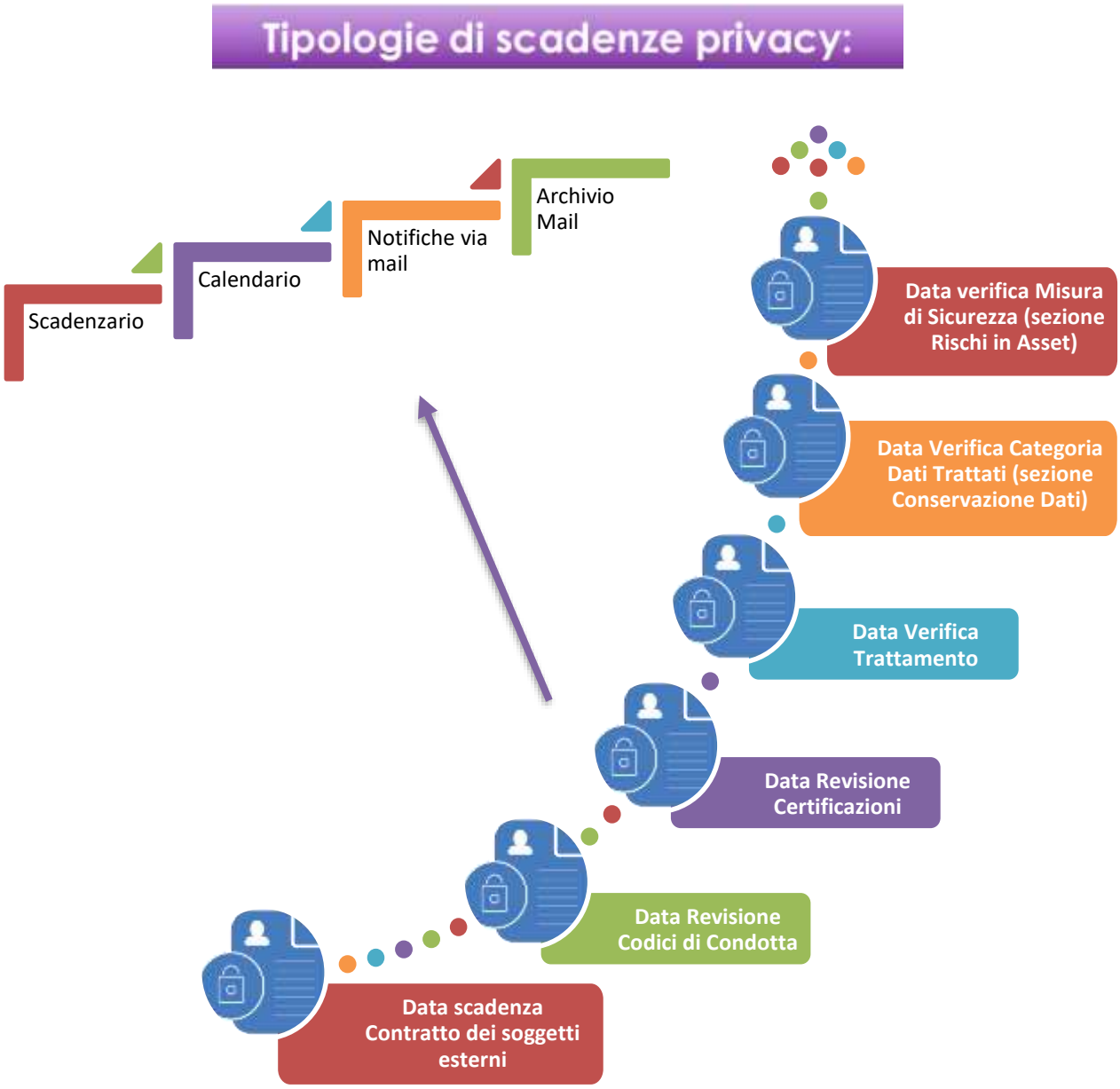
Per accedere a tale sezione, selezionare, dalla Home, la voce corrispondente.
Da tale sezione, è possibile procedere, quindi, alla stampa del **registro trattamenti** sia per Titolare del trattamento che per Responsabile del trattamento, come previsto dal regolamento.

È possibile stampare il registro delle attività del trattamento secondo il modello semplificato per le PMI predisposto dal garante privacy.

Nella sezione "Registro trattamento", dalla finestra di dialogo che si apre, selezionare registro per titolare del trattamento o responsabile del trattamento e mettere il segno di spunta su modello semplificato: verrà generato un registro in formato .xls secondo il modello messo a disposizione dal garante della privacy.



2.5 GESTIONE SCADENZE



Il sistema permette di gestire tutte le scadenze che riguardano la privacy sopra elencate, attraverso:

- lo **scadenzario**, accessibile dalla colonna opzioni presente all'interno del back office;
- il **calendario**
- il **gestore delle notifiche** presente nel menu Admin
- il **gestore delle mail** presente nel menu Admin

Per maggiori dettagli si rimanda al manuale completo di ***SICURWEB***:

https://www.sgslweb.it/wp-content/uploads/file/Manuale_SicurWEB.pdf

Capitolo 3 SEZIONE D.P.I.A.

3.1 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI – INTRODUZIONE AL NUOVO REGOLAMENTO EUROPEO GDPR

Il nuovo regolamento europeo introduce un concetto importante di *accountability* (responsabilizzazione) del titolare del trattamento secondo il quale egli è tenuto a mettere in atto delle politiche che tengano conto costantemente del rischio che un determinato trattamento dei dati personale può comportare per i diritti e le libertà degli interessati.

Secondo quanto previsto dall'**art.35** del GDPR, quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, i titolari sono obbligati a svolgere una valutazione di impatto, prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative, da loro stessi individuate per mitigare l'impatto del trattamento, non siano ritenute sufficienti, cioè quando il rischio residuale per i diritti e le libertà resti elevato.

*"…Una **valutazione di impatto** sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli…"* [1].

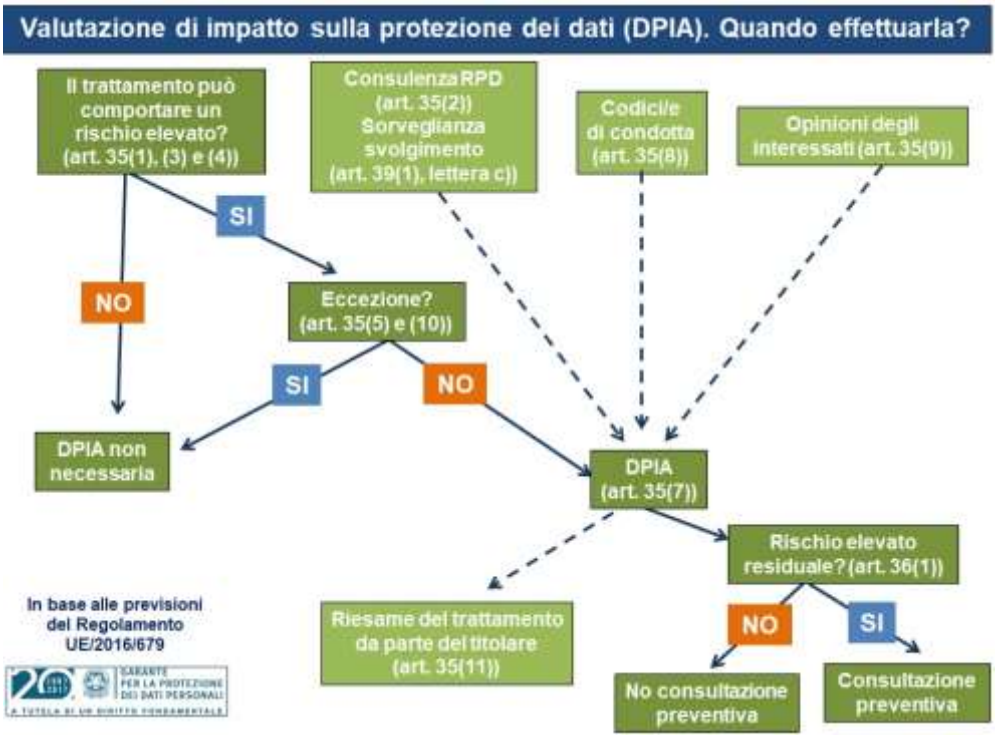


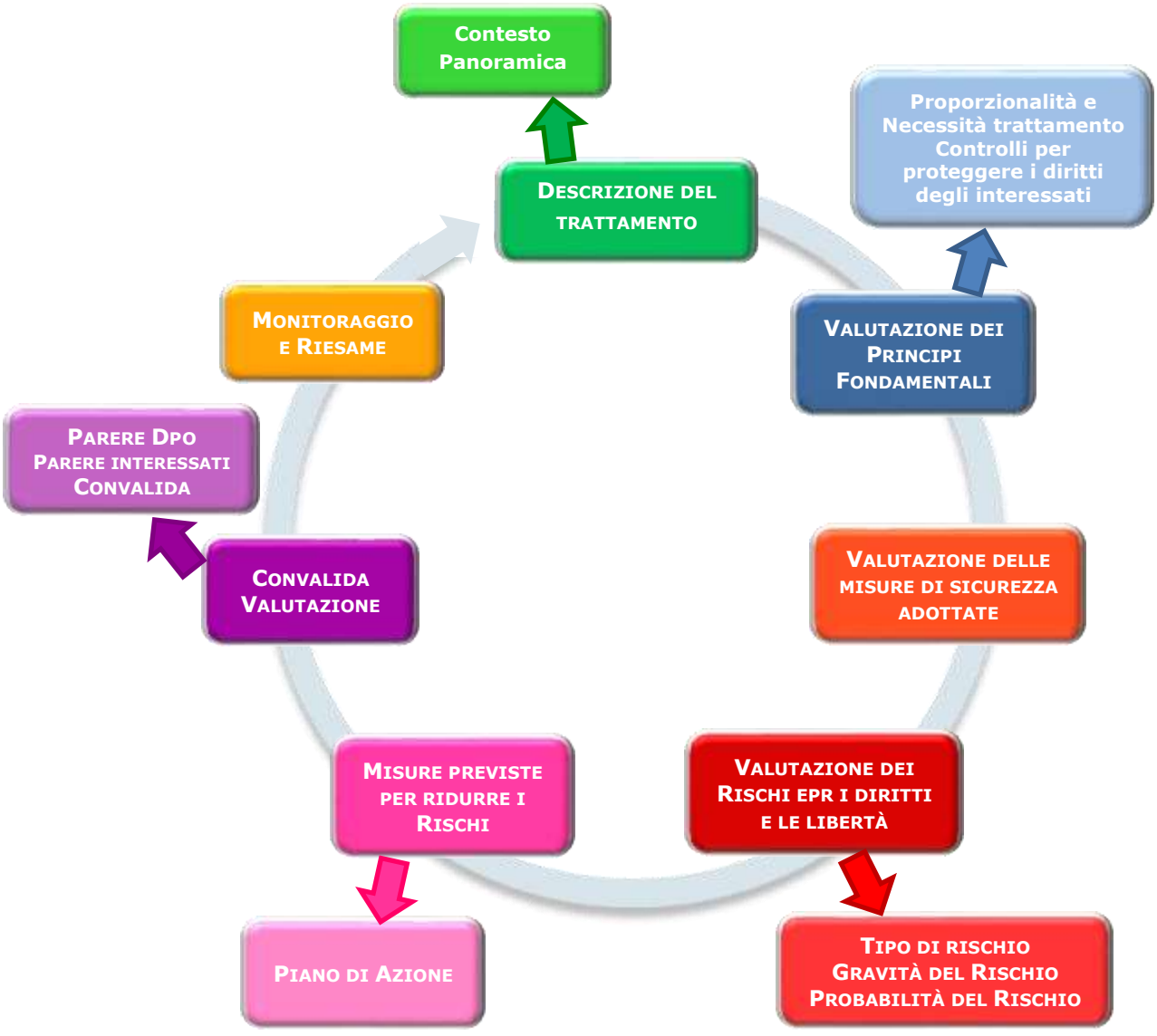
Immagine e dettagli sono disponibili sul sito del garante per la privacy alla pagina web: https://www.garanteprivacy.it/regolamentoue/DPIA

[1] [Gruppo di lavoro WP 248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679]

"*…Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati…"* (rif.: **comma 2 art. 32** Regolamento UE/2016/679 "sicurezza del trattamento").

Per maggiori dettagli consultare la pagina web:
www.sgslweb.it/2018/05/25/gdprivacy-valutazione/

3.2 SCHEMA DI FLUSSO DI UNA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI



Nel seguente flusso di processo, di una valutazione di impatto, va tenuto presente che ognuna delle fasi può essere riesaminata più volte, prima di procedere ad una convalida finale della stessa.

3.3 METODOLOGIA USATA PER LA VALUTAZIONE DI IMPATTO

La sezione della D.P.I.A. si basa sul modello del software del CNIL (*Commission Nationale de l'informatique et des libertés*), l'Autorità francese per la protezione dei dati, che offre un percorso guidato alla realizzazione della D.P.I.A., secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle "Linee-guida sulla DPIA" e compatibile con gli standard internazionali sulla gestione del rischio (ad esempio ISO 31000).

"…In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

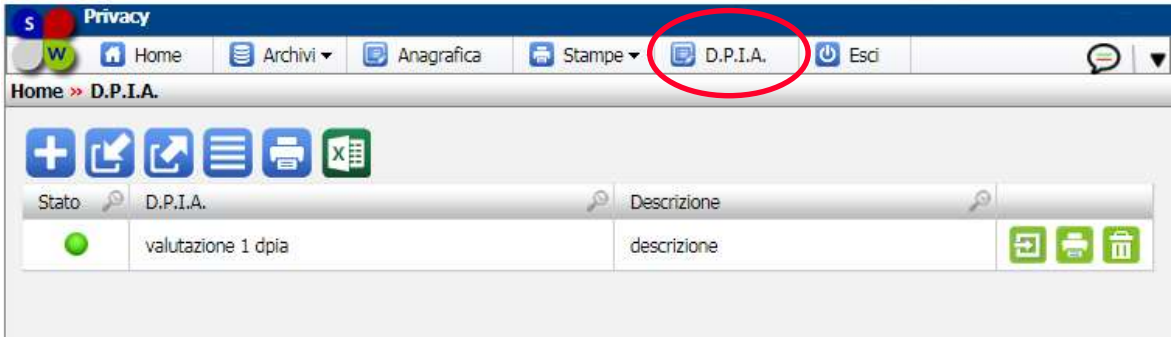
- ***stabilendo il contesto**: "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- ***valutando i rischi**: "valutare la particolare probabilità e gravità del rischio";*
- ***trattando i rischi**: "attenuando tale rischio" e "assicurando la protezione dei dati personali", e "dimostrando la conformità al presente regolamento"* [2].

Tale modello è stato riconosciuto, dal Garante della Privacy, come un valido strumento a supporto del titolare e del responsabile del trattamento per effettuare una valutazione del rischio ed è stato tradotto anche in lingua italiana con la collaborazione del nostro Garante.

Il vantaggio della DPIA, come strutturata in SICURWEB, rispetto al software del CNIL, è la possibilità di richiamare gran parte dei dati, necessari per la valutazione, dal flusso precedentemente creato.

3.4 ACCESSO ALLA D.P.I.A.

Per accedere a tale sezione, selezionare dalla barra dei menu la voce **D.P.I.A.**: si apre così la seguente schermata, dalla quale è possibile creare e lavorare su una valutazione di impatto.



Nella parte superiore della finestra, sotto la voce Home>>D.P.I.A., sono presenti, in ordine, i seguenti comandi:

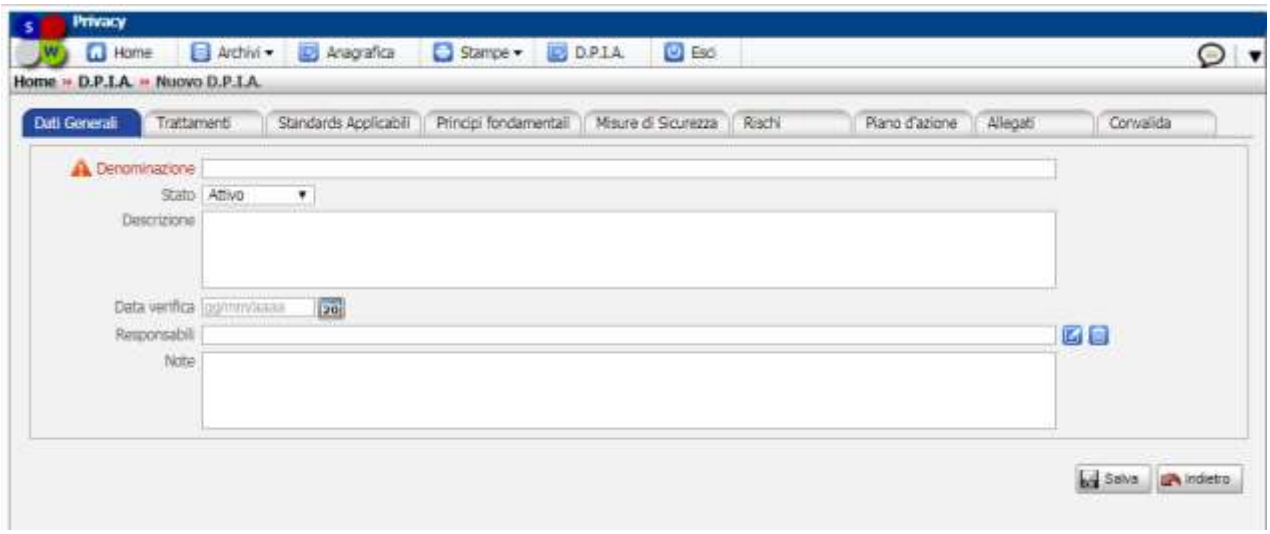
- **Nuova D.P.I.A.**: tale comando permette di creare una nuova DPIA;
- **Importa D.P.I.A.**: permette di importare, sotto forma di un file ".xml", all'interno di un'unità organizzativa una singola valutazione o un insieme di valutazioni, create, in un'altra unità organizzativa;

[2][Gruppo di lavoro WP 248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679]

- **Esporta D.P.I.A.**: permette di esportare una singola valutazione o un insieme di valutazioni, create in un'unità organizzativa, salvando un file ".xml" che potrà poi essere importato all'interno di un'altra unità organizzativa;
- **Mostra revocati**: visualizza le valutazioni revocate;
- **Stampa**: permette di stampare i dati riportati a video;
- **Stampa tabella**: permette di estrapolare, in un file excel, i dati riportati a video;

3.4.1. CREAZIONE DI UNA NUOVA DPIA

Per creare una **nuova DPIA**, selezionare il comando "Nuova DPIA"; si aprirà una schermata suddivisa in più schede, come mostrato nella figura seguente:

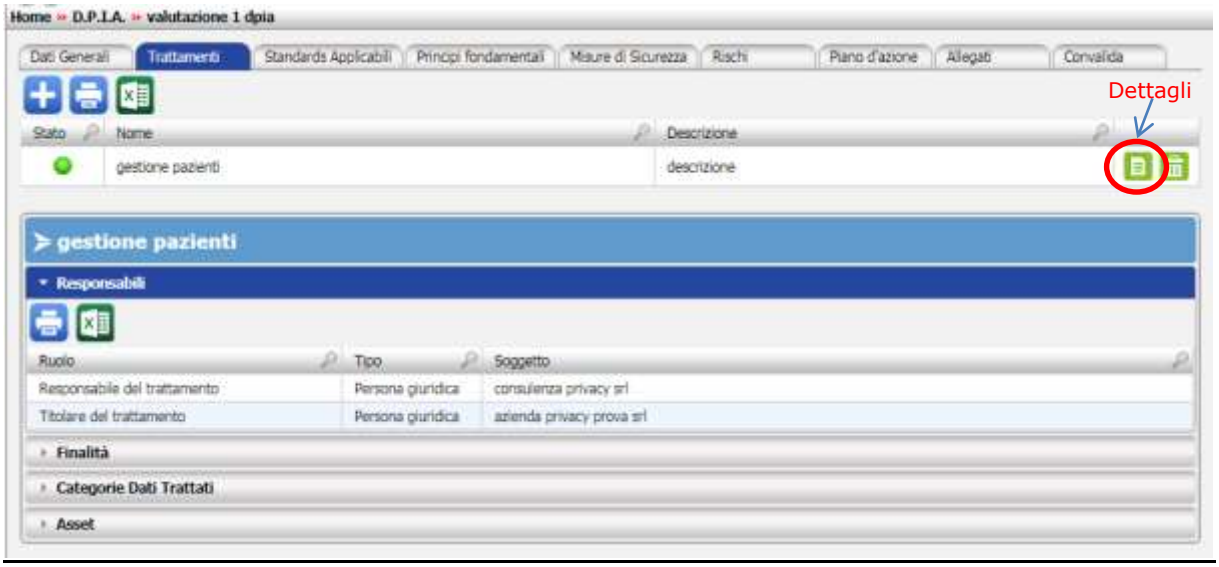


Per procedere alla realizzazione della valutazione, bisogna compilare le singole schede.

Dalla prima scheda "**DATI GENERALI**" è necessario inserire il **nome** della valutazione, una **descrizione**, la **data di verifica**, che permetterà di monitorare e aggiornare tale valutazione attraverso un riesame continuo e una rivalutazione regolare, ed eventuali **responsabili** specifici (ad esempio, a seconda delle politiche, dei processi e delle norme interne, eventuali consulenti indipendenti come avvocati, esperti informatici, esperte di sicurezza etc.).

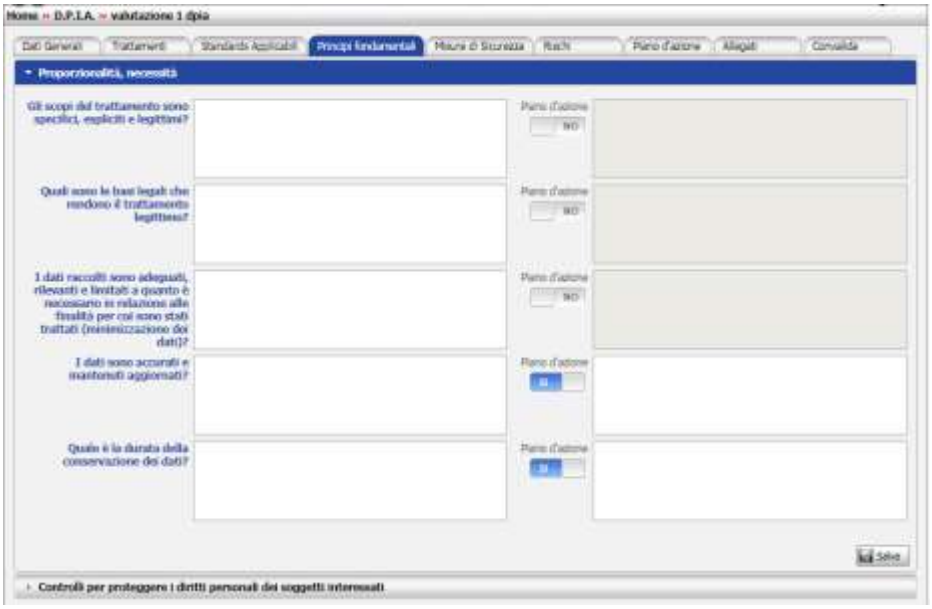
Inserite queste informazioni, salvare i dati: viene, così creata la nuova valutazione e ci si può spostare nella scheda "**TRATTAMENTI**".
All'interno di questa scheda, è possibile importare, dalla finestra di dialogo che si apre utilizzando il tasto "nuovo" , il trattamento o come previsto dal GDPR anche più trattamenti simili che presentano rischi elevati analoghi. Importando i trattamenti, in automatico, saranno richiamate, nella valutazione, tutte le informazioni precedentemente individuate sul singolo trattamento: responsabili, finalità, categorie dei dati trattati e gli asset con associate le misure di sicurezza.

Per visualizzare tali informazioni, basta aprire la sezione dei dettagli, attraverso l'apposito tasto "dettagli" situato a destra di ogni riga come illustrato nella figura seguente.



Dalla scheda successiva "**STARDARDS APPLICABILI**" è possibile richiamare eventuali codici di condotta o certificazioni legati al trattamento o ai trattamenti che si stanno valutando, e che sono stati inseriti, precedentemente, nella sezione corrispondente.
Il rispetto di un codice di condotta o l'adozione di eventuali certificazioni sono utili al fine di dimostrare che sono state messe in atto, relativamente ai trattamenti effettuati, misure adeguate e conformi al nuovo regolamento europeo sulla protezione dei dati.

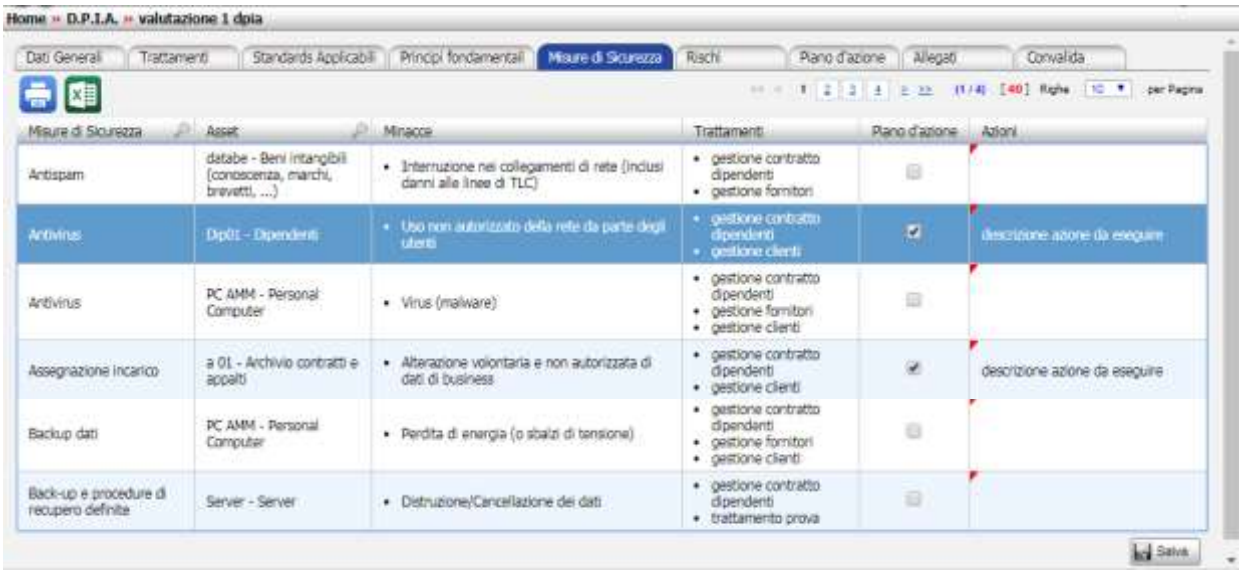
Nella scheda "**PRINCIPI FONDAMENTALI**" si dovrà procedere ad una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità. Per fare ciò, si dovranno compilare le due sezioni presenti all'interno della scheda: una sezione relativa alla "**proporzionalità e necessita**" del trattamento e l'altra riferita ai "**controlli per proteggere i diritti personali dei soggetti interessati**".



Per ogni sezione, è presente una serie di domande che permette di eseguire una valutazione e di individuare eventuali piani di miglioramento. Per inserire un piano di azione, basterà mettere il flag sul **SI** e nella casella, che si attiva a destra, dettagliare le azioni da effettuare.

Tutte le azione di miglioramento individuate, saranno inserite nel piano di azione.

Nella scheda "**MISURE DI SICUREZZA**", l'applicativo si richiama, in automatico, tutte le misure di sicurezza individuate all'interno degli asset associati ai trattamenti che si stanno valutando. Sarà, quindi, possibile individuare delle azioni di miglioramento per ognuna di tali misure di sicurezza: per fare ciò, mettere il segno di spunta nella casella "piano di azione" e procedere, nella casella al fianco, a dettagliare tali azioni.
Tutte le azione di miglioramento individuate, saranno inserite nel piano di azione.



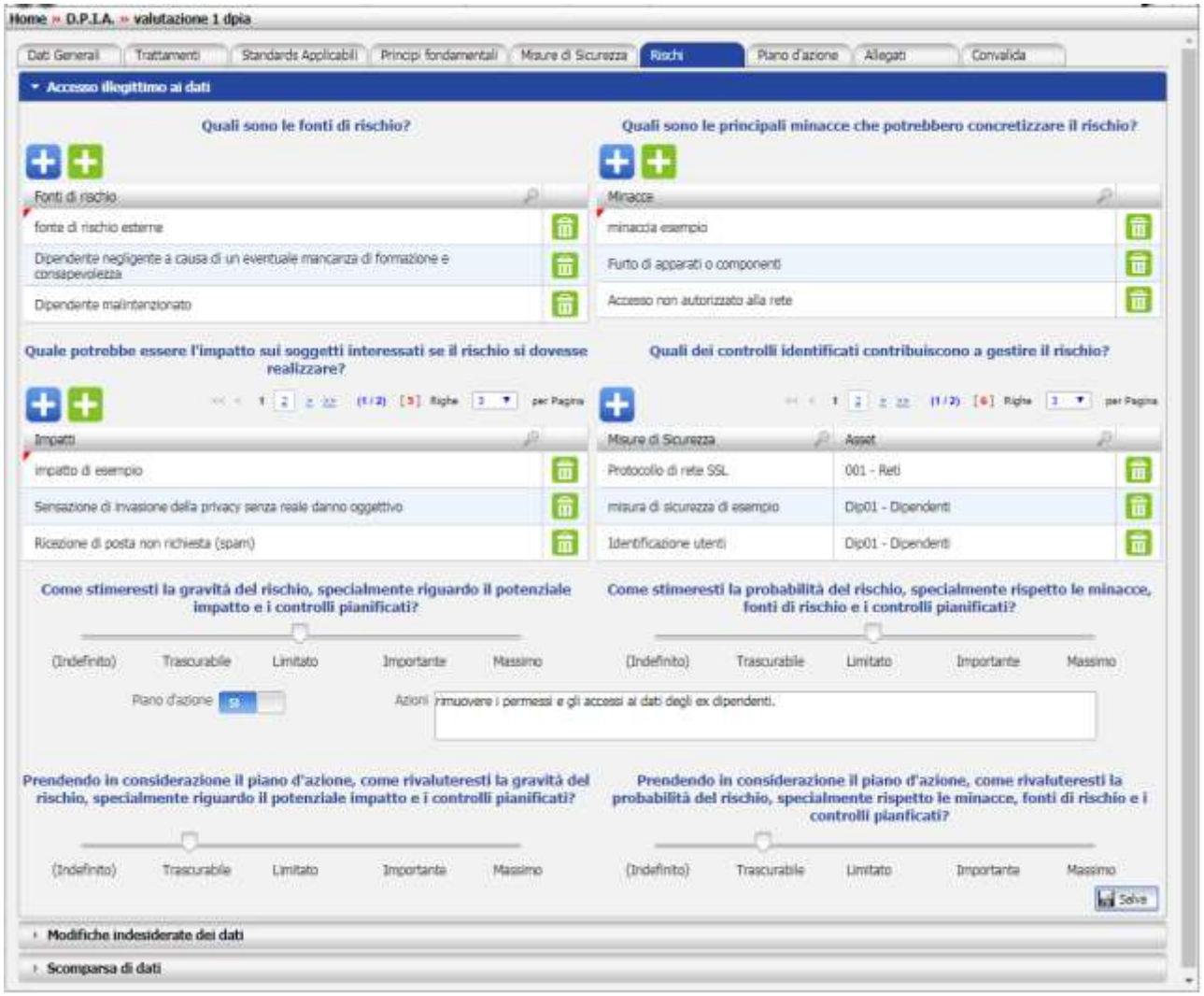
Completata anche questa scheda, ci si sposta in "**RISCHI**"; tale scheda è suddivisa in tre sezioni, ciascuna delle quali permette di eseguire un processo di valutazione dei rischi per la privacy legati al trattamento dei dati personali e cioè:

- **Accesso illegittimo dei dati**
- **Modifiche indesiderate dei dati**
- **Scomparsa dei dati**

Tale valutazione va eseguita dal punto di vista dell'interessato, individuando i potenziali impatti negativi che il verificarsi di uno di questi tre rischi possa comportare per i diritti e le libertà degli interessati stessi. In modo particolare, tale valutazione deve comprendere l'origine, la natura, la particolarità e la gravità del rischio considerando le possibili fonti di rischio, le minacce che potrebbero determinare il verificarsi di tale rischio, gli impatti potenziali che il verificarsi del rischio comporta sugli interessati e le misure adottate per contenere tale rischio.

Per individuare le **Fonti di Rischio**, si può procedere o importando le stesse dall'archivio che si apre attraverso il tasto "importa" , oppure usando il comando "nuovo" che inserisce una nuova riga, all'interno della quale è possibile scrivere la fonte di rischio.
Per inserire le **Minacce** e gli **Impatti**, si può procedere nello stesso modo.
Vanno quindi individuate, tra le **misure di sicurezza** precedentemente adottate, quelle che contribuiscono a gestire il rischio in considerazione, cioè un accesso illegittimo ai dati.
Per fare ciò, è sufficiente importare, dalla finestra di dialogo che compare cliccando sul tasto "nuovo" , le misure di sicurezza adottate per mitigare il rischio in esame.

In base all'analisi appena eseguita, si dovrà, quindi, procedere alla **stima del rischio**: tale stima si base su una valutazione della **gravità** dello stesso rischio in base al potenziale impatto sugli interessati e ai controlli pianificati, e sulla valutazione della **probabilità** che il rischio si verifichi in base alle minacce, alle fonti di rischio e ai controlli pianificati.

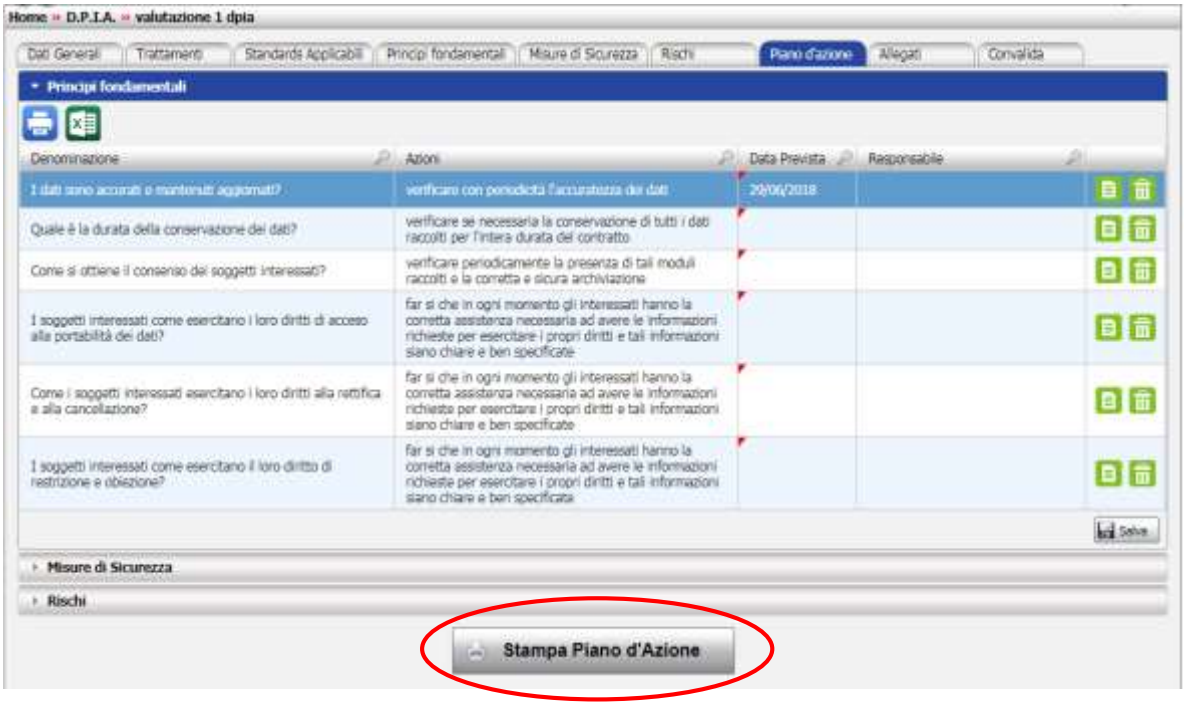


Per effettuare tale stima, bisogna spostare il cursore sul valore stimato per la gravità e per la probabilità.
Se risulta necessario, si potranno implementare misure aggiuntive per mitigare il rischio, nel qual caso basterà mettere il flag sul **SI** e nella casella, che si attiva a destra, dettagliare le azioni correttive da effettuare.

In base a queste azioni correttive, si procederà a una rivalutazione del rischio stimando come eventualmente è cambiata la gravità e la probabilità del rischio stesso a seguito delle azioni correttive individuate.

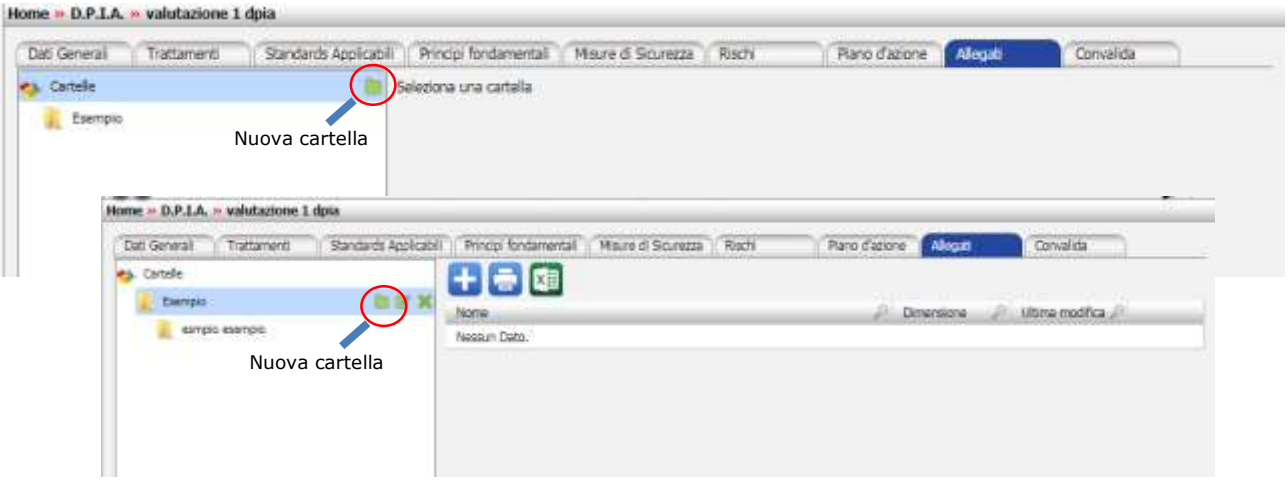
Completata tale sezione, si procederà ad eseguire una valutazione analoga prendendo in considerazione gli altri due possibili rischi, cioè una modfica indesiderata dei dati e una scomparsa dei dati; si procederà, cosi, come illustrato in precedenza, alla compliazione delle singole sezioni.

Dalla scheda che segue "**PIANO D'AZIONE**" saranno visibili tutte le azione di miglioramento che sono state individuate nelle tre schede precedenti; sarà quindi possibile pianificare in dettaglio l'implementazione di tutti i controlli aggiuntivi, inserendo la **data prevista** per ognuno di essi ed individuando eventuali **responsabili** importandoli dall'anagrafica che si apre cliccando sul comando "modifica" .

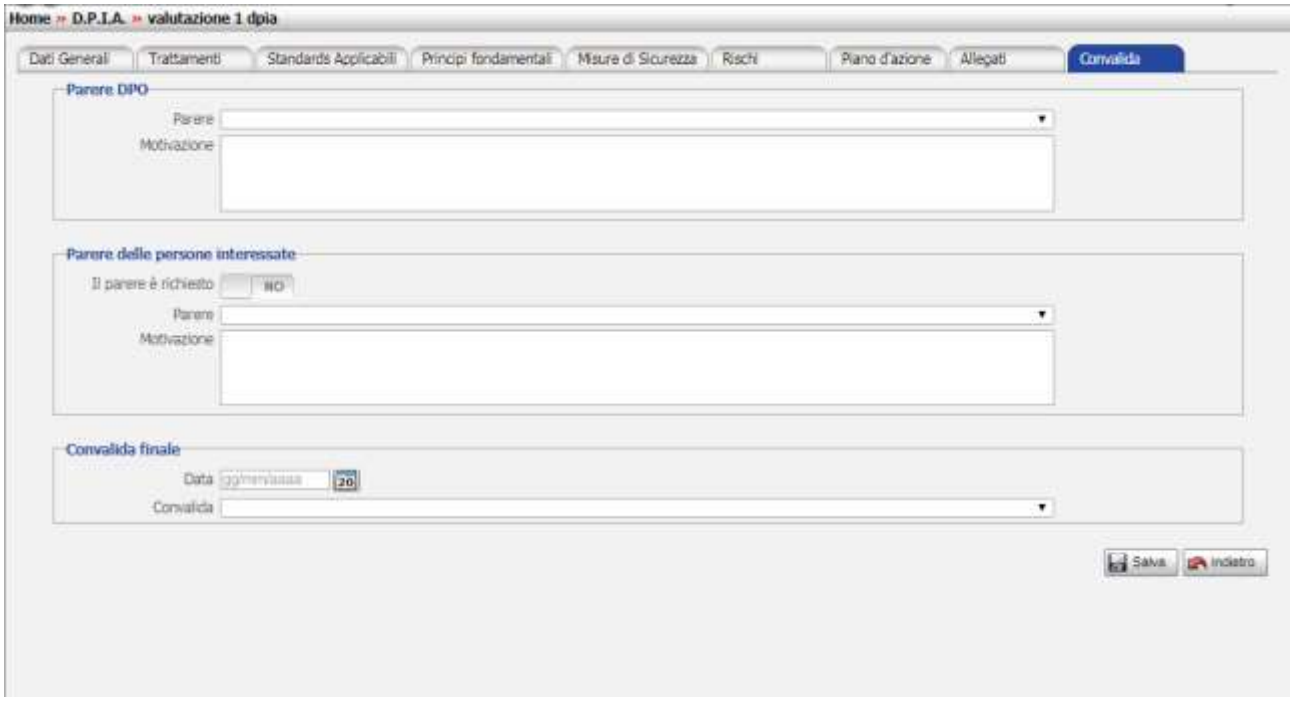


È poi possibile stampare il piano di azione attraverso l'apposito tasto di stampa.

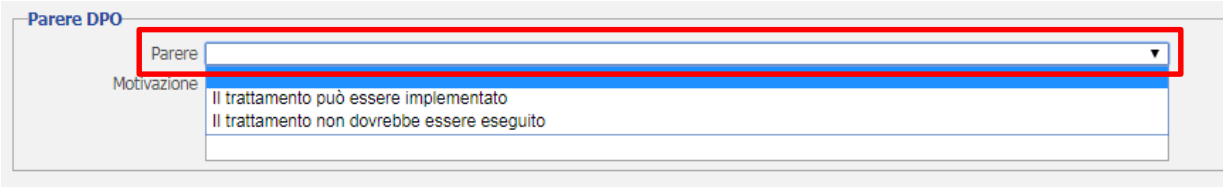
Nella scheda "**ALLEGATI"**, è invece possibile creare delle cartelle e sottocartelle e, per ognuna di esse, caricare all'intreno del sistema degli allegati. Create le cartelle e/o eventuali sotto cartelle utilizzando il pulsante "nuova cartella", sarà sufficiente cliccare sul comando "nuovo allegato" e, dalla finestra di dialogo che si apre, caricare il file.



Nell'ultima scheda "**CONVALIDA**" sarà possibile preparare e formalizzare la convalida della DPIA.

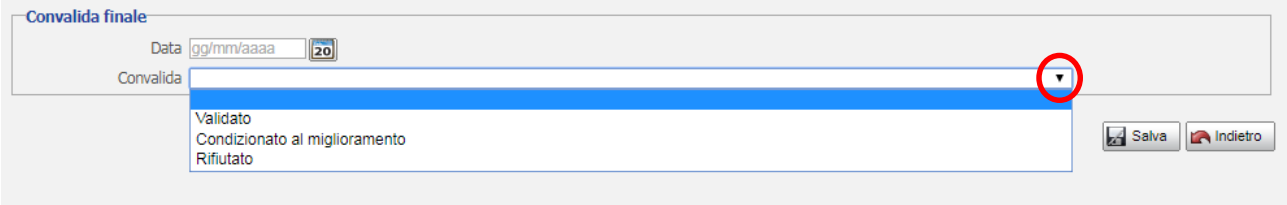


Per l'esecuzione della convalida, il titolare del trattamento dovrà consultare il responsabile della protezione dei dati (DPO/RPD), se nominato, il quale effettuato uno studio dell'intera DPIA, esprimerà il proprio parere, indicando se il trattamento può essere implementato oppure no e motivandone tale scelta. Tale "**parere**" andrà inserito nella casella corrispondente: cliccando sulla freccia posta a destra, si potrà selezionare la voce corrispondente al parere espresso. Nella sezione sottostante "**motivazione**" andrà dettagliata la motivazione di tale parere.



Nella sezione **parere delle persone interessate**, il titolare del trattamento valuterà se richiedere il parere degli interessati; in tal caso si deve mettere il flag sul **SI** e, raccolto tale parere, lo si riporterà nella casella corrispondente come spiegato nel caso del DPO e nella sezione sottostante "**motivazione**" si andrà a dettagliare la motivazione di tale parere.

Nell'ultima sezione, il titolare del trattamento, esaminato il parere del DPO ed eventualmente il parere degli interessati, procede alla convalidata del trattamento inserendo la **data** di tale convalida e l'esito della valutazione. Per inserire l'esito della valutazione, si procede selezionando lo **stato** della **convalida** dal menu che si apre cliccando sulla freccia posta a destra della casella corrispondente, come illustrato in figura.



A questo punto basterà salvare cliccando sul tasto "salva".
Cliccando poi sul tasto "indietro" si ritornerà alla schermata iniziale, dalla quale sarà possibile stampare l'intera valutazione, attraverso l'apposito tasto di **stampa**, riaprirla attraverso il tasto "**apri**" o eliminarla attraverso il tasto "elimina", in tal caso il sistema la metterà in uno stato revocato e sarà visibile solo cliccando sul pulsante "mostra revocati".

Le valutazioni di impatto, come i trattamenti e gli asset, possono essere esportate da un'unità organizzativa ed importate in un'altra.

Per esportare una o più valutazioni basterà selezionarle e, attraverso il tasto "esporta", si potrà salvare un file in ".xml" che potrà poi essere importato in altre unità organizzative attraverso il tasto "importa".