Documento di Progetto

Versione: 0.4 ***Data:***11/04/2019
Autore: Pellizzari Luca ***Responsabile:*** Baradel Luca

Indice

1. Introduzione 2
2. Descrizione della soluzione proposta 2
   2.1. Sketch Home page 2
3. Vincoli 3
4. Login e logout 4
5. Registri 5
   5.1. Registro dei trattamenti 6
   5.2. Registro dei soggetti autorizzati al trattamento 6
   5.3. Registro degli eventi di potenziale violazione della privacy 6
6. Gestione degli eventi 7
   6.1. Sketch eventi 8
7. Segnalazioni 10
   7.1 Sketch segnalazioni 11
8. Gestore Documenti 11

Modifiche	Versione	Autore	Data
Creato documento	0.1	Baradel Luca	12/12/2018
Modificati casi d'uso e riorganizzata struttura	0.2	Baradel Luca	05/01/2019
Riorganizzata struttura	0.3	Baradel Luca	17/01/2019
Aggiunti sketch	0.4	Pellizzari Luca	11/04/2019

1. Introduzione

Nel presente documento viene proposta una soluzione software per la gestione della privacy in tutti gli aspetti specificati dal cliente la cui definizione dei termini tecnici o relativi al regolamento è presente nel documento che contiene il glossario. La soluzione è organizzata in sezioni in cui vi è una prima descrizione iniziale e successivamente una presentazione delle proposte degli aspetti chiave e delle possibili soluzioni dal punto di vista dell'utente finale. Al fine di rendere più leggibile all'utente gli schemi vengono di seguito spiegati i significati delle parole `<<include>>` e `<<extend>>`:

- `<<include>>` rappresenta le azioni specifiche e obbligatorie che devono essere eseguite ogniqualvolta viene eseguita l'azione principale. È leggibile come "l'azione primaria A include le funzioni secondarie A1, A2, ecc.";
- `<<extend>>` rappresenta le azioni opzionali possibili relative ad un determinato comportamento, esse, come dice il nome "estendono il comportamento di un'azione". È leggibile come "eseguendo l'azione primaria B è anche possibile eseguire B1, B2, ecc.".

2. Descrizione della soluzione proposta

La soluzione consiste in una web-application accessibile da browser dal personale amministrativo incaricato dell'inserimento e gestione dei dati presenti all'interno del sistema. L'applicazione risiede in un server attivo ventiquattro ore su ventiquattro per permettere l'accesso al portale in qualsiasi momento, all'interno di esso i dati vengono memorizzati in un database accessibile solamente attraverso l'applicazione. L'accesso all'applicazione da browser avviene, come specificato, dalle persone autorizzate che dispongono delle credenziali di accesso fornite ai responsabili. Nelle sezioni successive vengono descritte nel dettaglio le operazioni effettuabili dall'utente e un diagramma dei casi d'uso.

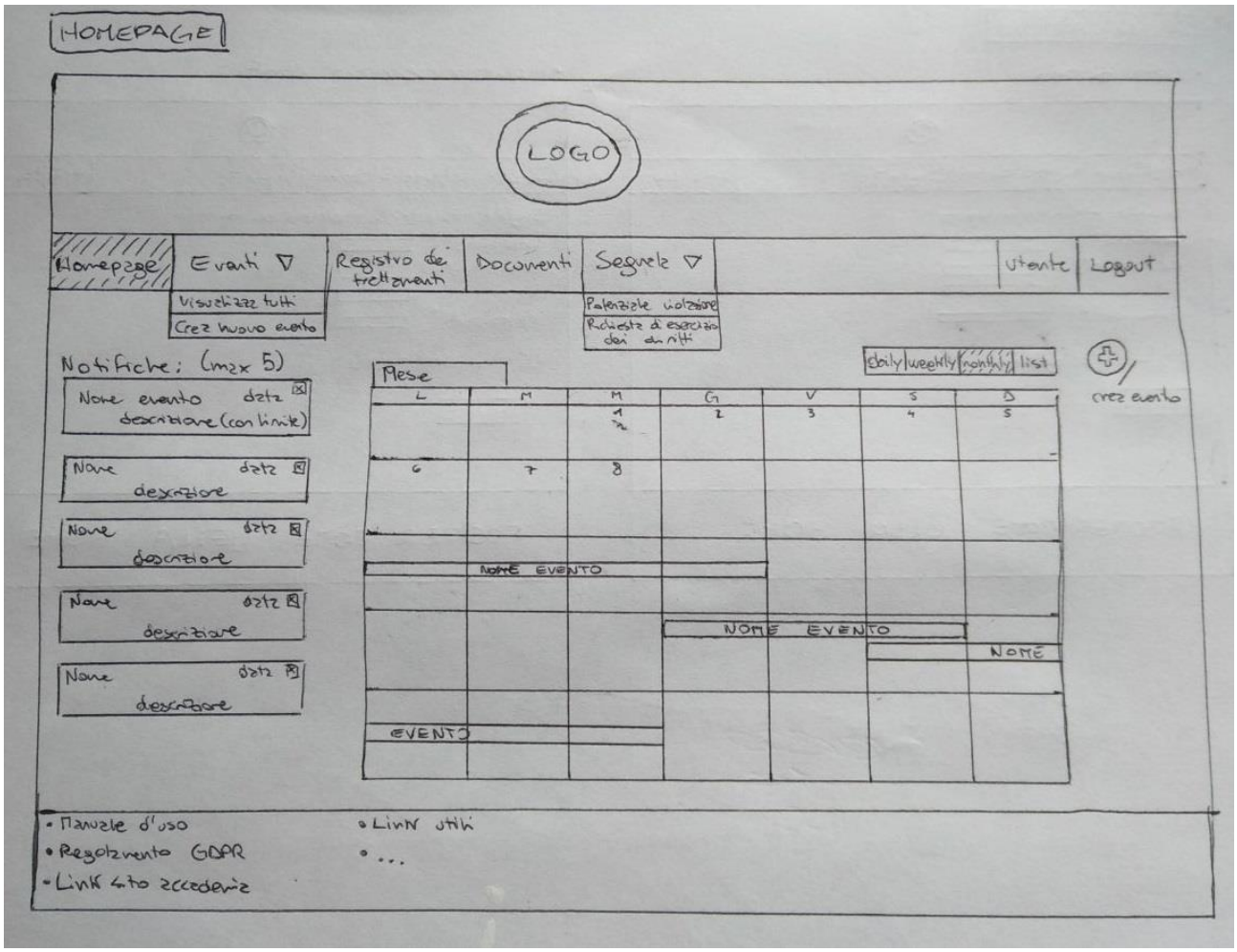
L'utente rappresenta la persona fisica autorizzata che interagisce con il sistema. Un utente può accedere al sistema inserendo le credenziali fornitegli dall'*amministratore*[1] del sistema da qualsiasi piattaforma connessa ad internet. Egli può inserire, modificare e cancellare dati nelle tabelle descritte di seguito, l'utente può inoltre filtrare e ricercare i dati oppure ordinarli secondo uno dei campi presenti.

2.1. Sketch Home page

Di seguito viene mostrato uno sketch per la struttura scelta per la home page dell'applicazione:

- in alto abbiamo una barra che contiene il logo dell'Accademia;
- successivamente abbiamo una barra di navigazione che ci dice in quale sezione dell'applicazione ci troviamo (è evidenziata la home page) e ci dà la possibilità di spostarci nelle altre sezioni tramite un comodo click;
- nella parte centrale dello schermo troviamo due delle funzionalità principali dell'applicazione: sulla destra la sezione che mostra le notifiche e sulla sinistra il calendario;
- in fondo alla pagina invece troviamo alcuni link utili come ad esempio il sito dell'Accademia, il regolamento GDPR e il manuale utente.

[1] L'*amministratore* di sistema rappresenta la persona responsabile del sistema, in grado di interagire direttamente con il server senza passare dall'applicazione.



3. Vincoli

Il cliente ha posto due vincoli principali per quanto riguarda tempo e budget:

- La soluzione deve essere completata e consegnata entro 6 mesi dal primo incontro con il cliente;
- Il budget del cliente per la soluzione ammonta ad un totale di €10.000.

4. Login e logout

L'accesso all'applicazione viene effettuato attraverso una pagina di login che verifica le credenziali inserite dall'utente. Un utente riceve le sue credenziali dall'amministratore del sistema, ad ogni persona autorizzata vengono forniti dati diversi in modo che il login all'applicazione comporta un'identificazione univoca dell'utilizzatore così da poter inserire automaticamente i dati di quest'ultimo dove richiesti. È fortemente consigliato effettuare il logout dall'applicazione una volta terminate tutte le operazioni effettuabili. Questo comporta un'uscita sicura senza lasciare operazioni in sospeso e previene eventuali scambi di account o intrusioni di terzi al sistema.

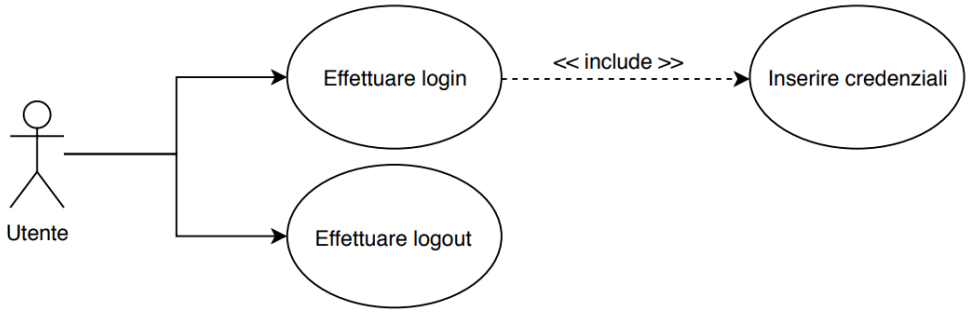


Figura 1 – Casi d'uso nel login

5. Registri

In questa sezione vengono descritti i principali registri presenti all'interno del sistema, essi sono il registro dei trattamenti, il registro dei soggetti autorizzati al trattamento e il registro degli eventi di potenziale violazione di privacy. Queste due componenti sono visualizzate come delle tabelle che rappresentano i dati salvati nel database dell'applicazione. In ognuno dei registri sono disponibili funzionalità di ordinamento, filtraggio e ricerca di determinati elementi. È possibile, successivamente ad una ricerca o filtraggio, scaricare i soli allegati relativi ai dati filtrati.

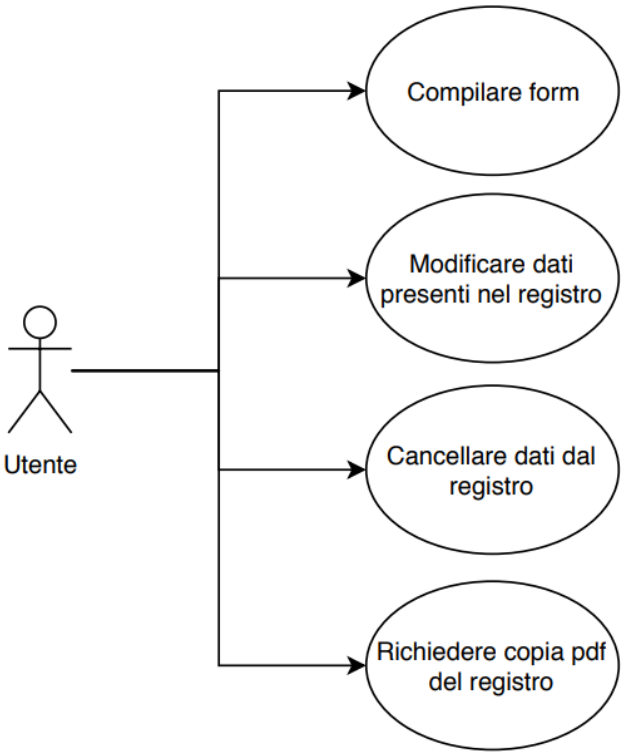


Figura 2 – Casi d'uso dei registri

5.1. Registro dei trattamenti

Dalla pagina principale sarà disponibile un tasto per l'accesso al registro dei trattamenti, in questa sezione sarà disponibile un tasto per l'inserimento di un nuovo trattamento, che porterà ad un form che richiede l'inserimento di tutti i dati specificati eccetto quelli dell'utente che sono registrati automaticamente al momento della sottoscrizione. Ogni trattamento nella tabella avrà un tasto che porta alla pagina per la modifica di esso, un tasto per scaricare eventuali allegati presenti nel gestore dei documenti e un tasto per richiedere il download in formato .pdf del trattamento. In questa tabella vengono memorizzati automaticamente i dati dell'utente che effettua la registrazione di un nuovo trattamento, e tutti i dati analizzati nell'analisi dei requisiti e dal modello di registro dei trattamenti fornito dal cliente, in unione ad un campo per eventuali allegati presenti nel gestore dei documenti. È possibile che per un eventuale trattamento esterno ci sia un link al registro dei soggetti autorizzati al trattamento per la visualizzazione delle informazioni relative al responsabile esterno.

5.2. Registro dei soggetti autorizzati al trattamento

Il registro dei soggetti autorizzati al trattamento viene rappresentato, come il registro dei trattamenti, da una tabella che visualizza i dati salvati nel database, i campi ad essa associati saranno quelli specificati dal cliente e ricavati dai modelli forniti dallo stesso, sarà inoltre presente una sezione relativa ai responsabili esterni e alle relative nomine, in questa sezione saranno disponibili i file del gestore documenti, accessibili tramite appositi link. Questa sezione è accessibile dal registro dei trattamenti stesso tramite un tasto specifico oppure da un link presente all'interno del registro dei trattamenti che filtra automaticamente la tabella. A sua volta il registro dei soggetti autorizzati al trattamento possiede un campo che fa riferimento al registro dei trattamenti in cui sarà presente un link che riporta al registro dei trattamenti filtrando la pagina a seconda del soggetto autorizzato. È possibile aggiungere dati all'interno di questo registro tramite un apposito form che prevedere l'inserimento di tutti i dati richiesti e il caricamento di eventuali allegati, tali allegati verranno automaticamente caricati nel gestore dei documenti.

5.3. Registro degli eventi di potenziale violazione della privacy

Il registro degli eventi di potenziale violazione della privacy è rappresentato come i precedenti da una tabella, verrà compilato automaticamente un nuovo form al momento della dichiarazione di una possibile violazione e i dati saranno salvati all'interno del database, contemporaneamente verranno automaticamente inviate delle e-mail di notifica all'autorità incaricata e agli interessati. Alla scadenza di questo evento verrà notificata la necessità di completare il record con i dati mancanti. Da questa sezione è possibile scaricare eventuali documenti di segnalazione presenti all'interno del gestore dei documenti.

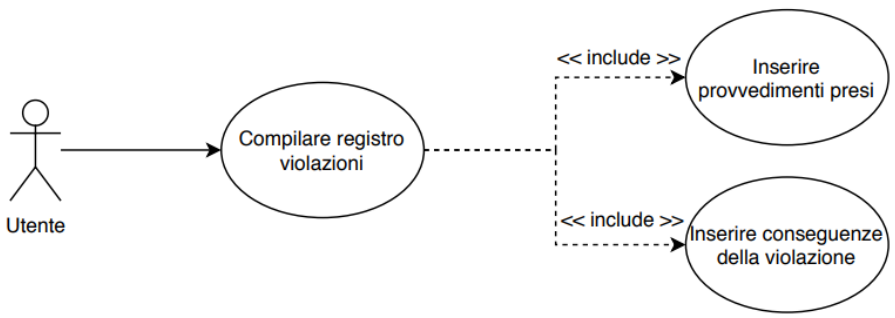


Figura 3 – Casi d'uso del registro degli eventi di potenziale violazione della privacy

6. Gestione degli eventi

L'utente dalla pagina iniziale ha accesso ad un calendario elettronico nel quale sono memorizzati tutti gli eventi registrati automaticamente dal sistema oppure creati arbitrariamente dagli utenti. Dalla pagina iniziale viene visualizzato il titolo e la data dell'evento temporalmente più prossimo. Il calendario elettronico viene visualizzato come un classico calendario nella forma di una tabella rappresentante il mese corrente. È possibile navigare il calendario per poter visualizzare eventi passati o eventi futuri. Nella stessa è pagina è presente un tasto per l'inserimento di un nuovo evento o l'inserimento di una nuova tipologia di evento. Un evento è caratterizzato da una tipologia predefinita, un titolo, una data e ora, una descrizione ed eventualmente da un elenco di partecipanti, sono presenti inoltre campi modificabili per fornire più dettagli che comprendono stato dell'evento, classe (che identifica se l'evento è un task oppure un evento standard), tipo (che indica il fine dell'evento con una parola chiave), note e eventuali tempi di inserimento, termine o tempo di inizio effettivo. Il calendario notificherà automaticamente gli eventuali partecipanti oppure tutto il personale con una notifica nella pagina iniziale un certo intervallo di tempo precedente al suo inizio. Tale notifica condurrà direttamente all'evento. Un evento può essere modificato, modificando i dati sopra citati, oppure cancellato.

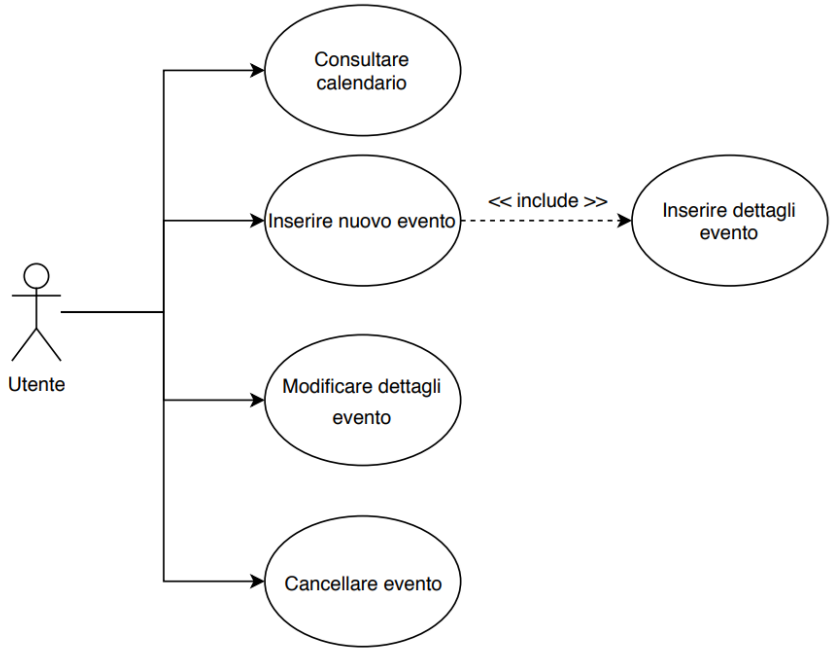


Figura 4 – Casi d'uso nella gestione degli eventi

Una tipologia di evento rappresenta un set di informazioni che verrà attribuita ad un evento. Una tipologia di evento può essere definita durante la creazione di un evento o dalla pagina del calendario. Per definire tale tipologia è necessario specificare i tempi di notifica (ossia con quanta precedenza l'evento verrà notificato), la priorità della notifica (specifica quanto evidente sarà la notifica di tale evento, ad esempio un evento con bassa priorità verrà notificato con un pallino rosso nella schermata iniziale nella sezione degli eventi, mentre un evento importante verrà notificato con una notifica pop-up che richiede attenzione immediata e non può essere ignorata) e un'eventuale periodicità (ossia una ripetizione dell'evento in un certo lasso di tempo e un certo numero di volte). Gli eventi che hanno come tipologia "Richiesta esercizio diritti" o "Data Breach" saranno gestiti autonomamente dal sistema quindi non sarà possibile inserire eventi appartenenti ad una delle due tipologie sopra citate.

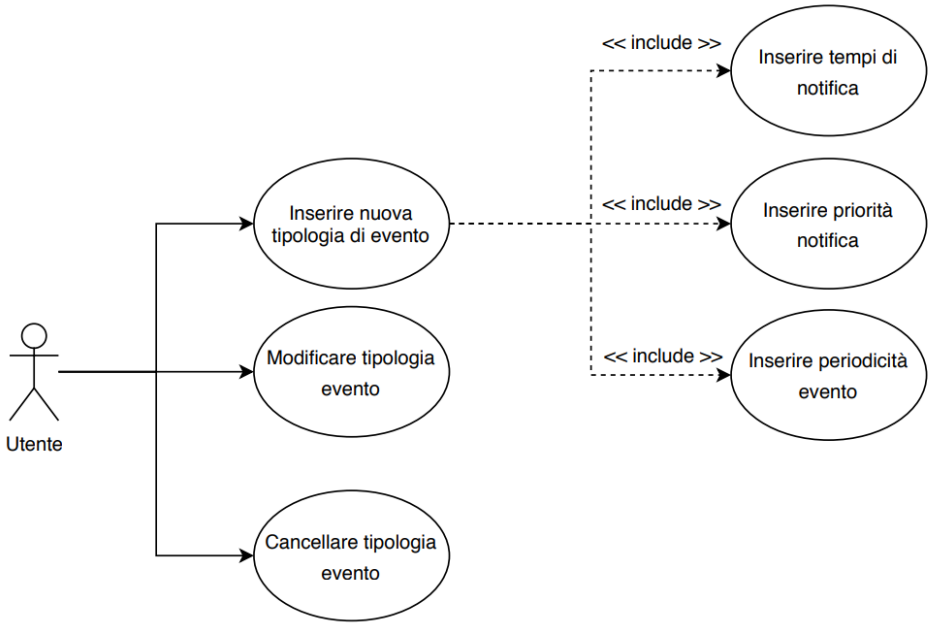
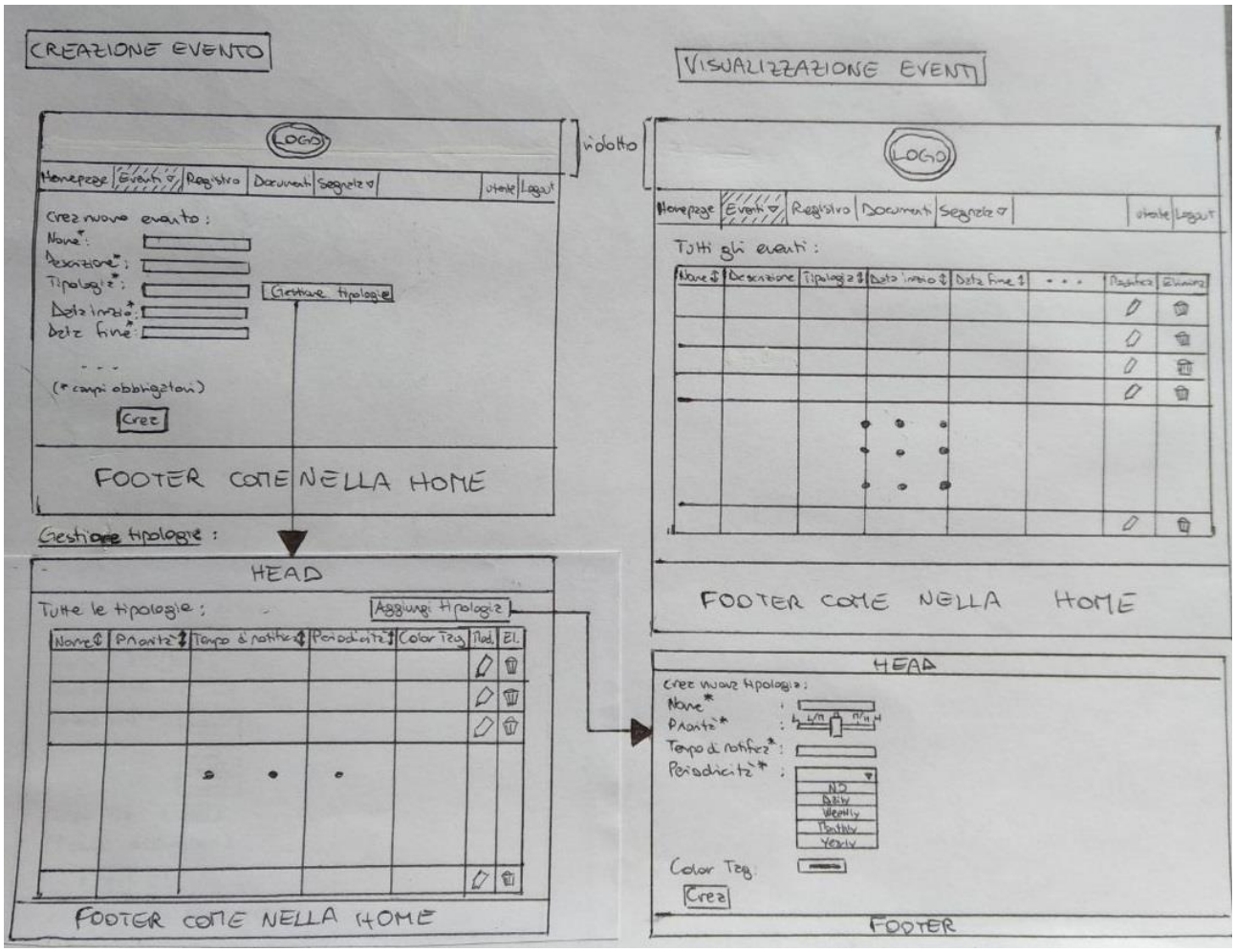


Figura 5 – Casi d'uso nella gestione di una tipologia di evento

6.1. Sketch eventi

Di seguito viene mostrata una possibile implementazione (prototipo a bassa fedeltà di una delle schermate dell'applicazione) per le operazioni appena descritte quindi:

- Inserimento di un evento tramite form;
- Visualizzazione dei dettagli di un evento;
- Modifica/cancellazione di un evento;
- Inserimento di una nuova tipologia di evento tramite form;
- Visualizzazione dei dettagli di una tipologia di evento;
- Modifica/cancellazione di una tipologia di evento.


CREAZIONE EVENTO
VISUALIZZAZIONE EVENTI
LOGO
Homepage
Eventi
Registro
Documenti
Segnala
utente
Logout
Crea nuovo evento:
Nome*:
Descrizione*:
Tipologia*:
Data inizio*:
Data fine*:
(* campi obbligatori)
Crea
Gestisci tipologie
FOOTER COME NELLA HOME
Tutti gli eventi:
Nome
Descrizione
Tipologia
Data inizio
Data fine
Modifica
Elimina
Gestione tipologie:
HEAD
Tutte le tipologie:
Aggiungi tipologia
Nome
Priorità
Tempo di notifica
Periodicità
Color Tag
Mod.
El.
Crea nuova tipologia:
Nome*
Priorità*
Tempo di notifica*
Periodicità*
NO
Daily
Weekly
Monthly
Yearly
Color Tag
Crea
FOOTER

7. Segnalazioni

Le segnalazioni possono essere di due tipi: “Richiesta esercizio diritti” oppure “Data breach”. In caso di data breach l’utente è tenuto a registrare una potenziale violazione dei dati, per farlo nella home page c’è una sezione per la creazione di una potenziale violazione. Essa consiste in un form nel quale verranno specificati il tipo di violazione, la data e quali dati sono a rischio. La registrazione della violazione crea automaticamente un evento con tipologia “Data breach” seguendo strettamente le tempistiche specificate dal committente, inoltre viene creato automaticamente uno score all’interno del registro degli eventi di potenziale violazione della privacy. Verrà inoltre creato un evento che notificherà la necessità di completare lo score con i dati relativi a conseguenze, provvedimenti ed altro. Il caso della richiesta di esercizio dei diritti è analogo, cambia solo il tipo dei dati che andranno inseriti all’interno del form; per quanto riguarda le notifiche il sistema si comporterà come appena descritto per un data breach, solo che i tempi di notifica saranno diversi.

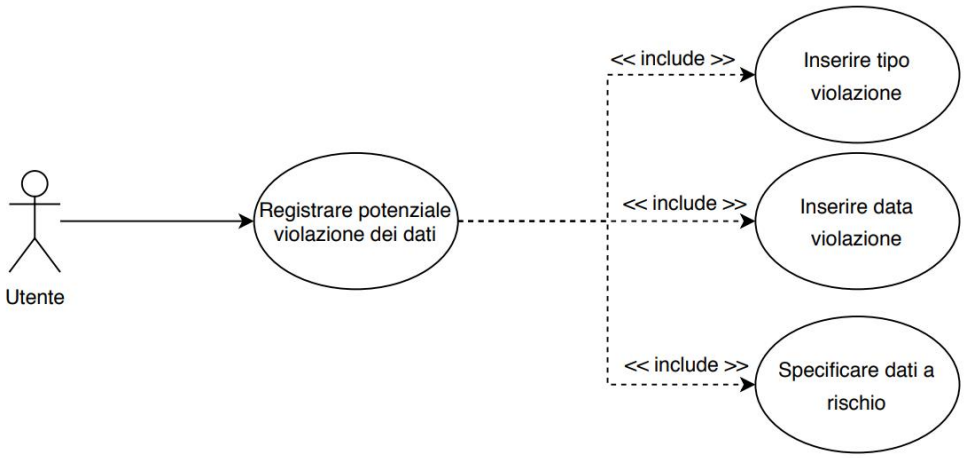
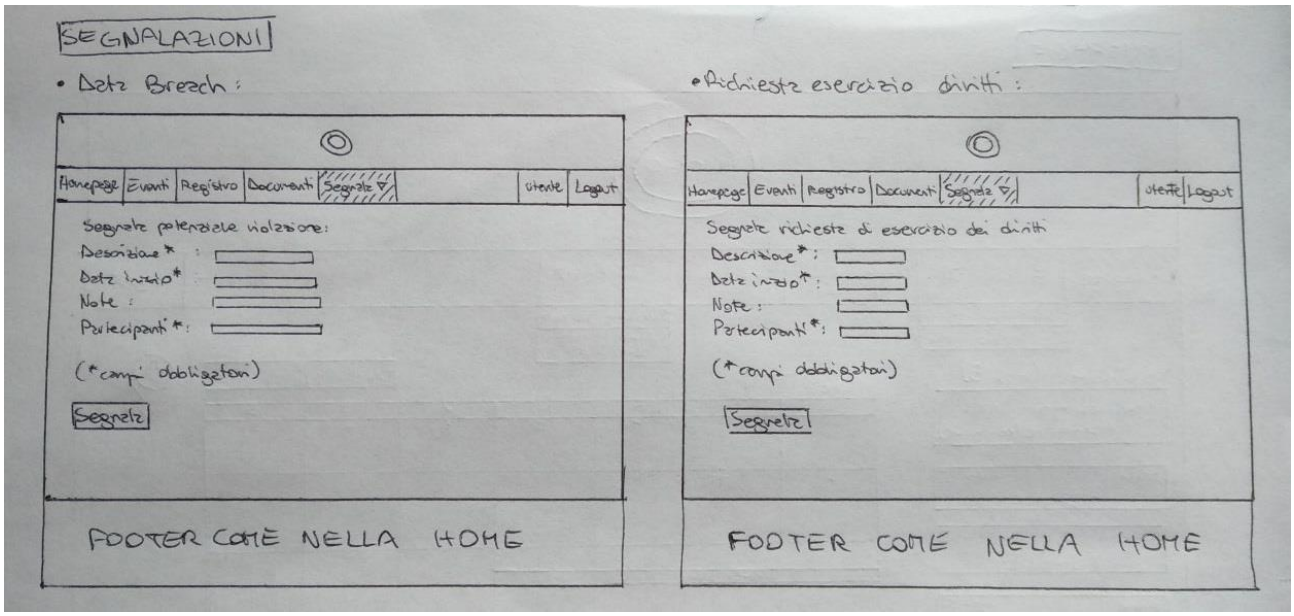


Figura 6 – Casi d’uso della gestione in caso di data breach

7.1 Sketch segnalazioni

Come descritto nella sezione "7. Segnalazioni" abbiamo a disposizione due form che ci permettono di inserire una segnalazione per le due tipologie di evento "Data breach" e "Richiesta di esercizio dei diritti". In questo prototipo non sono mostrati tutti i possibili campi che possiamo inserire all'interno del form, lo scopo dello sketch infatti è solo quello di mostrare un'anteprima del design dell'applicazione. Inoltre, c'è da notare che le tipologie di evento per le segnalazioni sono già selezionate quindi non viene richiesto all'utente di inserirle manualmente.



8. Gestore Documenti

Il mantenimento della documentazione che descrive il sistema e tutti i manuali relativi alle procedure interne sono salvati come file all'interno dell'applicazione. All'interno del gestore sono presenti anche le informative della privacy e un archivio dei documenti di nomina. Questi file possono essere versionati, gestiti con operazioni di aggiornamento o cancellazione oppure inseriti nel gestore in modo da renderli

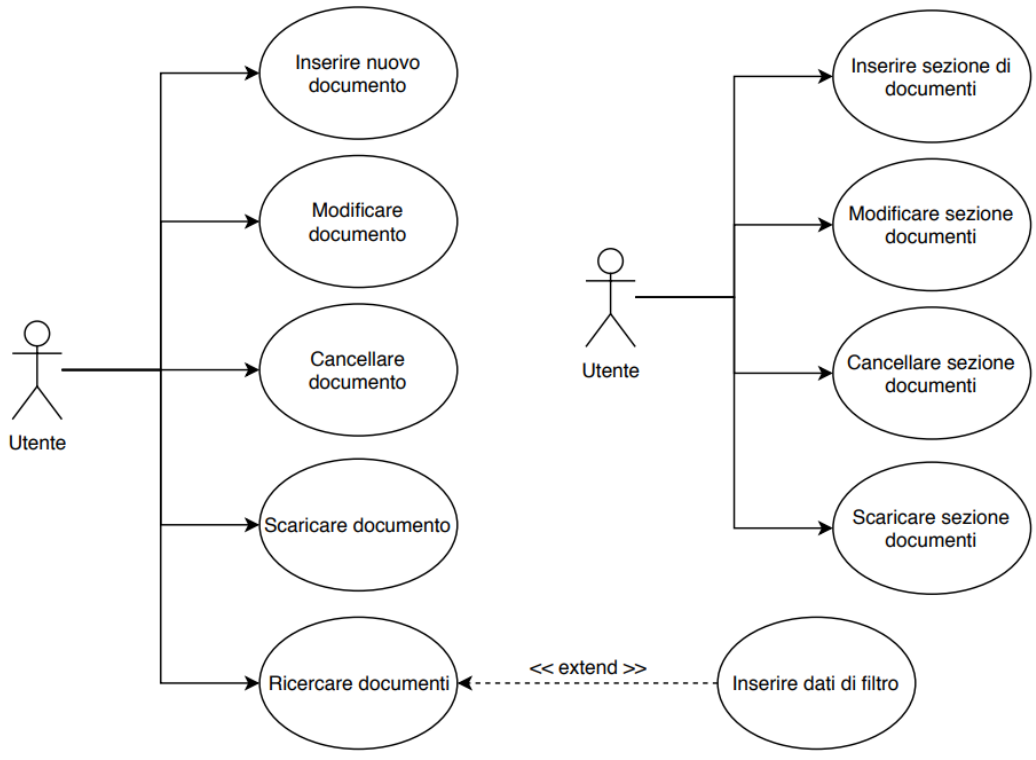


Figura 7 – Casi d'uso del gestore dei documenti

disponibili. Questo gestore permette la creazione di sezione e di fornire dei tag ai file in modo da rendere semplice la ricerca e il filtraggio dei file. È disponibili anche la possibilità di creare, modificare e cancellare sezioni, in cui è possibile archiviare i file per ordinarli visivamente e creando una gerarchia. È possibile, inoltre, scaricare tutti i file relativi ad un tag o ad una sezione.