

Introduzione

L'obiettivo è costruire un sistema finalizzato alla tutela dei dati personali, conforme alla normativa GDPR, per l'Accademia delle Belle Arti di Udine.

Requisiti funzionali: stakeholder: cliente.

- R1.** Il sistema deve consentire di tenere il registro dei trattamenti, ovvero di gestire i documenti in cui vengono registrati i processi dove si trattano dati personali. I registri saranno riempiti autonomamente dal personale autorizzato, il sistema non deve entrare nel merito dei processi eseguiti, ma deve permettere l'aggiunta, l'accesso, la modifica e l'eliminazione dei dati nel registro. Il sistema deve inoltre consentire di ricercare e selezionare elementi in base a determinati attributi di questi (tipo/autore del processo, interessati, ...).
- R2.** Il sistema deve permettere di gestire task ed eventi, mostrandoli in un calendario delle attività. Deve essere possibile inserire nuovi eventi o task, con i relativi attributi (classe, tipo, frequenza, data di inserimento, data di termine previsto, data di termine effettivo, riferimenti anagrafici, descrizione e note), modificarne i dettagli associati oppure cancellarli. Il sistema deve inoltre notificare l'utente all'avvicinarsi di determinati eventi, permettendogli quindi di impostare la finestra temporale entro cui ricevere gli avvisi. Il calendario va visualizzato come una griglia in cui sono elencati i giorni di ogni mese e gli eventi/task associati e deve essere possibile filtrare le varie attività in base allo stato (aperto, in scadenza o scaduto) ed alla tipologia.
- R3.** Il sistema deve consentire di gestire i data breach, permettendo agli utenti di registrare questi eventi, inserendo la tipologia di violazione, la data di questa e i dati a rischio. Inoltre deve agevolare l'invio delle notifiche della violazione al garante e agli interessati entro 3 giorni dalla notifica della violazione.
- R4.** Il sistema deve registrare autore, data e contenuto delle richieste di esercizio dei diritti degli interessati, registrare le risposte date e sapere che la richiesta è stata evasa. Se ciò non avviene entro 20 giorni deve generare alert evidenti.
- R5.** Il sistema deve consentire la gestione di varia documentazione, permettendo di inserire, modificare, cancellare, scaricare, accedere e ricercare documenti, i quali sono distinti sulla base di: tipo (informative, modelli, nomine, manuali, ...), data di creazione, data di modifica, descrizione, stato e soggetto. È opportuno che il sistema consenta di archiviare i documenti in base alla tipologia, permettendo agli utenti di inserire, modificare o cancellare sezioni di documenti ed eventualmente di scaricare tutti i documenti relativi ad una sezione.
- R6.** Il sistema deve permettere di gestire l'anagrafica, in cui si indicano i responsabili esterni ai trattamenti. Deve essere possibile registrare le nomine, indicandone stato e data e collegandovi i documenti di nomina associati.

Requisiti non funzionali: stakeholder: cliente.

Il sistema deve consentire un utilizzo sicuro e protetto delle funzionalità, ristretto ai membri del personale autorizzati: gli interessati non possono interagire con il sistema. Non sono stati specificati vincoli hw o di integrazione con altri sw.

Glossario

- **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a 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;

- **Dato personale** :qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Data breach**: 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;
- **Dati sensibili**: si considerano i dati personali come l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla vita sessuale o all'orientamento sessuale della persona, nonché dati genetici, dati biometrici, dati sulla salute e dati personali relativi a condanne penali o reati;
- **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- **Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.