Documento dei requisiti

Versione: 0.0.2 ***Data:*** 26/11/2018
Autore: Di Benedetto Gianluca ***Responsabile:*** Baradel Luca

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

R1. Il sistema deve consentire di tenere il registro dei trattamenti, ovvero registrare tutti i processi in cui si trattano dati personali, specificando l'autore del processo, quali dati sono trattati, di chi (qual è la categoria di interessato) e che tipo di dati, dove viene eseguito (interno o esterno), come viene eseguito (elettronico/cartaceo) e con che mezzo, descrivendo anche le finalità del trattamento. I processi possono essere specifici (richiesta iscrizione, iscrizione, esami, esame finale, manifestazioni, …) o trasversali per tutte le categorie interessate, ma in generale di qualsiasi tipo: i registri saranno riempiti autonomamente dal personale, è necessario un luogo in cui censire le procedure.

R2. Il sistema deve produrre una documentazione per ogni classe di interessato in cui si indica quali suoi dati vengono trattati, in quali processi, per quali scopi e per quanto tempo e le modalità di gestione. Deve inventariare le informative sulla privacy presentate agli interessati specificando data e versione e la presenza di consensi espliciti.

R3. R3. Il sistema deve calendarizzare le attività con cadenza periodica (controllo del sistema, attività di formazione, …) e marcarle una volta fatte, con la possibilità di allegare gli attestati.

R4. Il sistema deve mappare certi eventi e generare alert quando ci si avvicina alle scadenze

- R4.1. Richieste di esercizio dei diritti degli interessati: il sistema deve registrare autore, data e contenuto delle richieste, registrare le risposte date e sapere che la richiesta è stata evasa. Se ciò non avviene entro 20 giorni deve generare alert evidenti.
- R4.2. Data breach: quando vengono segnalati data breach, occorre stabilire entro 2 giorni se ci sia stata una violazione dei dati personali e attivare, entro 3 giorni dalla notifica della violazione, una comunicazione di questa al garante e all'interessato. Il sistema deve registrare l'evento e seguirlo strettamente in questi termini.

R5. Il sistema deve organizzare le nomine a responsabili esterni, inventariando i documenti di nomina e registrando che la nomina è stata fatta, a chi e in che data.

R6. Il sistema deve mantenere e rendere semplice l'accesso a tutti i manuali relativi alle procedure interne (che saranno definiti dal personale amministrativo). Inoltre deve mantenere tutta la documentazione che descrive il sistema, anche in termini di modelli di documenti da usare nei processi interni, e gli strumenti che si utilizzano.

Requisiti non funzionali

Il sistema deve consentire un utilizzo sicuro e protetto delle funzionalità, ristretto ai membri del personale: 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.