ANALISI DI CONFORMITÀ DEL SOFTWARE

Elenco preliminare documenti/informazioni

NOTE ALLA COMPILAZIONE

- **INSERIRE LE INFORMAZIONI RICHIESTE E FLAGGARE LE VOCI SUSSISTENTI**
- **NON FLAGGARE LE VOCI NON SUSSISTENTI**
- **LE DICHIARAZIONI RESE DEVONO ESSERE DIMOSTRABILI TECNICAMENTE E/O DOCUMENTALMENTE, SONO IRRILEVANTI PRASSI O CONSUETUDINI NON SCRITTE**
- **INVIARE ALL'INDIRIZZO DI RIFERIMENTO IL DOCUMENTO COMPILATO, UNITAMENTE ALL'EVENTUALE DOCUMENTAZIONE RICHIESTA, OVE APPLICABILE.**

SI PREGA DI INVIARE LA DOCUMENTAZIONE COMPLESSIVA TRAMITE CARTELLA .ZIP NOMINATA CON LA RAGIONE SOCIALE DELL'AZIENDA

LE INFORMAZIONI RICHIESTE SI RIFERISCONO SIA AGLI AMBIENTI DI SVILUPPO CHE DI PRODUZIONE DEL PRODOTTO OGGETTO DI ANALISI

1. DATI ANAGRAFICI

RAGIONE SOCIALE:

CONTATTO DI RIFERIMENTO:

2. DESCRIZIONE DELL'APPLICATIVO

2.1 Descrizione generale

Descrizione delle funzionalità dell'applicativo

Breve descrizione delle funzionalità e delle modalità operative del software

2.2 Sviluppo e utilizzo

Indicazione in merito alle modalità di sviluppo dell'applicativo ed agli usi che il Cliente intende farne

Software interamente sviluppato in autonomia (anche per mezzo di fornitori)

Customizzazione di Software licenziato

3. GOVERNANCE, MANAGEMENT E STAKEHOLDERS

Organigramma di Progetto

Indicare elenco ruoli delle figure coinvolte:

Profili di Autorizzazione

Documentazione in merito a come il Cliente decide come si costituiscono e gestiscono i profili di autorizzazione all'applicativo oggetto di analisi ed ai dati trattati tramite lo stesso.

Sussistenza nomina autorizzati alla gestione dei dati anche in via incidentale ed alla sicurezza dei dati *[se la casella è flaggata allegare il documento]*

Sussistenza policy gestione profili di autorizzazione (creazione, modifica, dismissione) *[se la casella è flaggata allegare il documento]*

Sussistenza profili di autorizzazione

3.1 Amministrazione di Sistema

Documentazione in merito a come il Cliente decide come si creano e gestiscono i profili di Amministrazione di Sistema (AdS) dell'applicativo oggetto di analisi.
Per Amministratore di Sistema si intendono figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti, incluse anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Sussistenza nomina a responsabile amministratori di sistema interni ed esterni *[se la casella è flaggata allegare il documento]*

Sussistenza nomine amministratori di sistema interni *[se la casella è flaggata allegare il documento]*

Sussistenza policy gestione nomine amministratori di sistema interni ed esterni *[se la casella è flaggata allegare il documento]*

Sussistenza di profili di amministrazione del sistema

Sussistenza sistema di loggatura AdS (log-in, log-out, inalterabili e cancellabili con conservazione almeno semestrale)

Sussistenza Relazione annuale in materia di AdS *[se la casella è flaggata allegare il documento]*

3.2 Data Protection Officer (DPO)

Documentazione in merito a come il Cliente ha deciso se adottare o meno il Data Protection Officer e, in caso positivo, documentazione disciplinante il ruolo del DPO in relazione al prodotto oggetto di analisi

Sussistenza documento di valutazione sul DPO *[se la casella è flaggata allegare il documento]*

Sussistenza nomina DPO (eventuale)

Sussistenza policy di gestione

3.3 Gestione fornitori

Documentazione in merito a come l'utilizzato procede alla valutazione preliminare di potenziali fornitori/collaboratori esterni e gestisce i rapporti contrattuali con fornitori/collaboratori e subfornitori rilevanti rispetto al software.

Sussistenza policy di selezione di fornitori/sviluppatori qualificati *[se la casella è flaggata allegare il documento]*

Sussistenza policy di gestione delle subforniture *[se la casella è flaggata allegare il documento]*

Contratto relativo alla erogazione del servizio da parte del fornitore

3.4 Training interno

Documentazione in merito alla formazione interna dei soggetti che sviluppano dell'applicativo oggetto di analisi.

Sussistenza attestazioni di formazione in ambito GDPR *[se la casella è flaggata allegare almeno un'attestazione]*

Sussistenza formazione in tema di sicurezza informatica rispetto alla tecnologia utilizzata

4. ACCOUNTABILITY, DESIGN E CONFIGURABILITA'

4.1 Elementi di privacy by design

Informazioni ed eventuale documentazione in merito a come il prodotto consente all'utilizzatore l'autonoma impostazione di determinate funzionalità del prodotto stesso.

Sussistenza settabilità di termini di cancellazione o anonimizzazione dei dati

Sussistenza audit tecnici sull'effettiva cancellazione o anonimizzazione dei dati se impostate

Sussistenza settabilità cifratura

Sussistenza audit sulle cifrature se impostate

Sussistenza settabilità pseudonimizzazione

Sussistenza audit sulle pseudonimizzazioni se impostate

Sussistenza settabilità delle impostazioni dei profili di autorizzazione

Sussistenza settabilità requisiti di complessità delle password di accesso

Sussistenza settabilità temporalizzazione della scadenza delle password

Sussistenza conservazione dello storico degli accessi

Sussistenza settabilità blocco utenza in caso di tentativi non andati a buon fine

Sussistenza settabilità time-out di sessione

In caso di sussistenza della tracciabilità delle operazioni svolte dagli accedenti all'applicativo, sussistenza della settabilità dei termini di cancellazione

Sussistenza strumenti di valutazione di bug

Sussistenza strumenti di debugging

Sussistenza policy di risoluzione dei bug rilevati

Sussistenza strumenti di monitoraggio data breach

Sussistenza di penetration test periodici

Lo strumento permette di storicizzazione le informative privacy rese agli interessati

Sussiste la possibilità di rettificare i dati

Sussiste la portabilità dei dati

E' applicabile il diritto di limitazione dei dati[1]

E' applicabile il diritto di cancellazione (cancellazione permanente dei dati)

4.2 *Ambiente di sviluppo*

Informazioni ed eventuale documentazione in merito a come il Cliente disciplina determinati elementi tecnici e/o procedurali relativi all'ambiente di sviluppo del prodotto oggetto di analisi.

[1] misure che consistono nel "contrassegnare" i dati personali conservati dall'utilizzatore che, a fronte di una richiesta dell'interessato, si trovi a dover in qualche modo riconoscere e segregare quei dati che non potrà più trattare in futuro. La limitazione deve essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

Sussistenza sistema di autenticazione

Sussistenza sistema di autorizzazione

Sussistenza di un sistema di controllo degli accessi logici

Sussistenza della conservazione in modo inalterabile e incancellabile dei log di accesso agli ambienti di sviluppo

Sussistenza storicizzazione di tutte le versioni delle implementazioni/personalizzazioni dello strumento

Sussistenza dello storico dei log delle modifiche apportate allo strumento

Sussistenza dell'identificabilità dell'autore delle modifiche apportate

Sussistenza di sistemi antintrusione logica

Sussistenza di canale protetto per lo sviluppo da remoto

Sussistenza di strong authentication per gli accessi da remoto all'area di sviluppo

In caso di rilascio di dati reali in ambiente di test, sussistenza di policy di cancellazione

Sussistenza policy di valutazione della sicurezza degli strumenti di terze parti inclusi open, free e librerie utilizzati per lo sviluppo

Sussistenza policy di recepimento degli aggiornamenti sugli strumenti di terze parti

5. CUSTOMIZZAZIONE E TESTING

Documentazione in merito a come il Cliente gestisce le personalizzazioni del prodotto oggetto di analisi.

Sussistenza policy recepimento richieste di customizzazione, di valutazione della customizzazione ed implementazione

Sussistenza policy di modalità e gestione testing

Sussistenza policy di effettuazione del penetration test sul prodotto customizzato

6. RILASCIO E COLLAUDO

Documentazione in merito a come viene gestita la messa in produzione del prodotto oggetto di analisi.

Sussistenza di policy per il rilascio del prodotto *[se la casella è flaggata allegare il documento]*

Sussistenza policy di gestione dei dati di test *[se la casella è flaggata allegare il documento]*

7. MANTENIMENTO E ASSISTENZA

Documentazione in merito a come viene gestito l'aggiornamento delle misure tecnico/organizzative adottate.

Processi di revisione delle policy implementate

Sussistenza policy relative alle DPIA *[se la casella è flaggata allegare il documento]*

8. DATA BREACH

Documentazione in merito a come sono prevenuti, valutati e gestiti eventuali violazioni di dati personali trattati per mezzo del prodotto oggetto di analisi o di sicurezza dei sistemi rilevanti rispetto al prodotto.

Sussistenza Documenti di classificazione del breach

Sussistenza di strumenti di prevenzione del breach

Sussistenza policy di notifica del data breach *[se la casella è flaggata allegare il documento]*

Sussistenza policy di contenimento e remediations del breach *[se la casella è flaggata allegare il documento]*

9. ALLEGATI

Allegare o inserire i campi del gestionale che raccolgono e contengono dati personali

Elenco campi contenenti dati personali