Dipartimento Tecnologie Informatiche

# Scheda check di compliance sicurezza e privacy applicativi software (V11)

| | |
|---|---|
| Denominazione software | |
| Codice software | |
| Fornitore | |
| Descrizione sintetica attività gestita | |
| Tecnologia | |
| Base dati | |

==========

**Le tabelle 1 e 2 definiscono le condizioni che richiedono accorgimenti specifici che saranno oggetto della proposta del fornitore nelle tabelle 3, 4 e 5.**

A. **Le tabelle 1 e 2 sono compilate preventivamente dal Collegio Tecnico per predeterminare il livello di rischio cui le misure richieste/offerte devono riferire.**

**Tabella 1 – Dati trattati dal software nel contesto di utilizzo**

| 1. **Tipologie dei dati gestiti mediante il prodotto software** | | |
|---|---|---|
| | SI | NO |
| - Il software gestisce dati Personali (identità, ruolo, qualifica, …) | X | |
| - Il software gestisce categorie particolari di dati personali | X | |
| - Il software gestisce dati relativi a condanne penali e reati | X | |
| - Il software gestisce dati a maggior tutela (HIV,IVG,…) | X | |
| 2. **Ambito di gestione del dato** | | |
| | SI | NO |
| - Sono gestiti dati relativi a episodi di cura | | |
| - Sono gestiti dati relativi a cittadini | X | |
| - Sono gestiti dati relativi a dipendenti (in quanto dipendenti dell'Azienda utilizzatrice) | X | |
| - Sono gestiti dati relativi a fornitori | | |
| - Sono conservati nel sistema documenti (esempio: PDF) che contengono dati personali e categorie particolari di dati personali e/o dati relativi a condanne penali o reati riferiti all'interessato (dati non disaccoppiabili) | X | |
| - E' richiesta/dispiegata una soluzione multi-aziendale | X | |

**Tabella 2 – Analisi del rischio**

**La valutazione di sintesi riporta il valore maggiore della riga / il valore maggiore della colonna (B<M<A<H)**

| Contesto | Livello di criticità | | | |
|---|---|---|---|---|
| | Riservatezza | Integrità | Disponibilità | Sintesi |
| Violazione di leggi, regolamenti o contratti | A | A | M | A |
| Violazione della privacy sui dati personali | A | A | M | A |
| Danni a persone | M | M | M | M |
| Blocco o ritardo nella erogazione di servizi aziendali o istituzionali | A | A | M | A |
| Effetti negativi nei rapporti con terze parti e danni all'immagine | A | A | M | A |
| Conseguenze finanziarie | M | M | M | M |
| | | | | |
| VALUTAZIONE DI SINTESI | A | A | M | A |

Criticità Bassa (B)-> il danno è trascurabile / lieve
Criticità Moderata (M)-> Il danno è limitato
Criticità Alta (A)-> Il danno è considerevole
Criticità molto alta (H)-> Il danno non è sostenibile

==========

**LEGENDA PER LA COMPILAZIONE DELLE TABELLE 3, 4 E 5**

| Colonna | Descrizione |
|---|---|
| **Obbligatoria** | **Compilata dal CT con una X.**<br>**La misura è ritenuta essenziale dall'Ente ai fini dell'ammissibilità tecnica della proposta, da valutare complessivamente in tutto il contesto dell'offerta tecnica ed eventuale Demo da cui sia possibile evincere il rispetto della normativa sul trattamento dei dati.** |
| **Fornitore (SI/NO)** | **Compilata dal fornitore con una X nella cella del SI o nella cella del NO (la casella non compilata vale NO).**<br>**Il fornitore attesta la presenza o meno della misura.**<br>**Misure offerte di compliance superiori si esprimono con una X sulla casella SI e una nota esplicativa nella tabella 5, riportando in quest'ultima il codice della riga (es. riportare <3.1-A> per riferire la prima misura della tabella 3)** |
| **Valutazione ESTAR** | **Comm. : la CG esprime con un SI o un NO la compliance della misura rispetto all'ambito.**<br>**Collaudo: In fase di collaudo si attesta la corretta implementazione della misura** |

**Tabella 3 – Compliance del software**

| 3. **Rispetto delle misure di sicurezza** | Obbligatoria | Fornitore | | Valutazione Estar | |
|---|---|---|---|---|---|
| | | SI | NO | Comm. | Collaudo |
| **3.1-A** Il software è integrato con sistemi di sicurezza permettendo la conformità al Regolamento Generale sulla protezione del dati 2016/679 necessarie per lo scenario d'impiego cui è destinato: Privacy by design; Privacy by default; minimizzazione; pseudonimizzazione. O comunque, Il software è parzialmente integrato con sistemi di sicurezza, tuttavia è possibile sviluppare dei controlli compensativi che permettono la conformità al Regolamento Generale sulla Protezione dei Dati n. 679/2016 necessarie per lo scenario di impiego cui è destinato.<br>**Se la risposta è SI, descrivere in tabella 5** | X | | | | |
| **3.2-A** Il software permette l'autenticazione degli utenti basata su tecniche di strong authentication (autenticazione basata su password ed OTP, SPID) | X | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **3.2-**B Il software permette l'autenticazione degli utenti tramite smart card (CNS, ecc.) | X | | | | |
| **3.2-C** Sono previste per default tecniche di abilitazione automatica di meccanismi di costruzione di password complesse | X | | | | |
| **3.2-D** Misure minime | | | | | |
| - La componente privata delle credenziali di accesso è di almeno 8 caratteri | X | | | | |
| - E' prevista l'obbligatorietà del cambio password al primo accesso (in quanto compatibile con il sistema di autenticazione offerto) | X | | | | |
| - E' prevista la modifica obbligatoria della password ogni 3 / 6 mesi (in quanto compatibile con il sistema di autenticazione offerto) | X | | | | |
| - E' prevista la disattivazione automatica dell'accesso all'applicativo dopo 6 mesi di non utilizzo o altro tempo parametrizzabile | X | | | | |
| - E' prevista la disconnessione della sessione dell'utente in caso di non uso dell'applicativo per un periodo di tempo parametrizzabile | X | | | | |
| **3.3** Il software tiene traccia (log accessi e log attività) delle operazioni effettuate tramite applicativo, comprese le attività di sola visualizzazione dei dati, per un tempo parametrizzabile e adeguato a quanto previsto da norme di legge e/o regolamenti (es. 24 mesi per il dossier sanitario) | X | | | | |
| **3.4** Il software permette la profilazione degli utenti (dipendenti autorizzati ad istruire le pratiche e quindi al trattamento dei relativi dati personali) in modo granulare da consentire solo la visibilità necessaria al ruolo svolto. | X | | | | |
| 4. **Rispetto delle misure e degli accorgimenti in tema di amministratori di sistema (per la parte di competenza del fornitore)** | **Obbligatoria** | **Fornitore** | | **Valutazione Estar** | |
| | | **SI** | **NO** | **Comm.** | **Collaudo** |
| - E' prevista la possibilità di creare livelli differenziati di amministrazione del sistema | X | | | | |
| - E' previsto un sistema di registrazione (access log) per gli accessi logici degli amministratori di sistema al database di supporto dell'applicativo | X | | | | |
| - Il sistema di access log ha caratteristiche di inalterabilità, completezza e di verifica della integrità dello stesso | X | | | | |
| - L'access log contiene almeno i riferimenti temporali, la descrizione dell'evento che le ha generate, l'identificazione del soggetto che ha compiuto l'accesso | X | | | | |
| - L'access log è conservato per almeno sei mesi o per il maggior tempo richiesto dalla normativa e/o da regolamenti (es. 24 mesi per il dossier sanitario) | | | | | |
| 5. **Misure specifiche per categorie particolari di dati personali o dati personali relativi a condanne penali e reati** | **Obbligatoria** | **Fornitore** | | **Valutazione Estar** | |
| | | **SI** | **NO** | **Comm.** | **Collaudo** |
| - I dati idonei a rivelare lo stato di salute e la vita sessuale/orientamento sessuale sono registrati e conservati separatamente dagli altri dati personali soggetti a trattamenti che non richiedono il loro utilizzo (disaccoppiamento) | X | | | | |
| - Il software consente l'adozione di tecniche di cifratura o di codici identificativi che non esplicitano direttamente il contenuto informativo in relazione alla gestione di dati idonei a rivelare lo stato di salute o la vita sessuale/orientamento sessuale. | X | | | | |
| - Il software consente l'adozione di tecniche di pseudonimizzazione in relazione alla gestione di categorie particolari di dati personali, o dati personali relativi a condanne penali o reati | | | | | |
| - Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante codici identificativi che non esplicitano direttamente il contenuto informativo | X | | | | |
| - Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, o documenti che contengono in modo non divisibile dati personali e categorie particolari di dati personali sono trattati mediante tecniche di cifratura | X | | | | |
| - Le categorie particolari di dati personali, o dati personali relativi a condanne penali o reati, sono trattati mediante altre soluzioni rispetto alle due precedenti, ai fini della loro temporanea inintelligibilità | | | | | |
| 6. **Diritto all'oblio** | **Obbligatoria** | **Fornitore** | | **Valutazione Estar** | |
| | | **SI** | **NO** | **Comm.** | **Collaudo** |
| - Il sistema consente di definire, per classi di informazioni, il tempo di conservazione | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | in relazione al momento in cui sono state prodotte e al momento in cui è stata raggiunta la finalità per le quali sono state raccolte. | | | | |
| - | Il sistema consente la cancellazione delle informazioni che hanno raggiunto il tempo limite di conservazione | | | | |
| - | Il sistema consente di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco | | | | |
| - | Il sistema dispone di servizi (esempio in collaborazione applicativa) che consentono ad un sistema esterno di individuare le informazioni relative ad un soggetto (interessato), e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco | | | | |
| 7. | **Funzione di repository sanitario /fascicolo sanitario /dossier sanitario** (Non compilare la sezione se la funzione non è richiesta in questa procedura) | **Obbligatoria** | **Fornitore** | | **Valutazione Estar** | |
| | | | **SI** | **NO** | **Comm.** | **Collaudo** |
| - | Il sistema consente di rilevare e tenere traccia temporalmente dei consensi e delle cessazioni di consenso, del paziente alla attivazione del suo FSE/DSE | | | | | |
| - | Il sistema consente il collegamento con sistemi esterni per acquisire l'esistenza o meno del consenso del paziente alla attivazione del suo FSE/DSE | | | | | |
| - | Il sistema consente l'accesso al FSE/DSE solo in relazione alla preventiva definizione del mandato assistenziale attivo (visita, ricovero, ecc. ) che ne giustifica l'utilizzo | | | | | |
| - | Il sistema consente di qualificare ogni singolo episodio di cura nello status deciso dal paziente relativamente al FSE/DSE (visibile, oscurato, oscuramento dell'oscuramento) | | | | | |
| - | Relativamente ai dati a maggior tutela, il sistema consente di identificarli e di rilevare lo specifico consenso del paziente ai fini del trattamento FSE/DSE | | | | | |
| - | Il sistema consente la visibilità dei dati alla sola struttura di appartenenza del sanitario in caso di non attivazione del FSE/DSE | | | | | |
| - | Il sistema tiene traccia degli accessi al FSE/DSE, rilevando i dati dell'operatore sanitario, della postazione di lavoro di accesso, della data e ora di accesso e delle azioni, anche di sola inquiry eseguite | | | | | |
| - | Il sistema consente l'accesso al sistema da parte del paziente tramite tessera sanitaria, al fine di operare sul proprio FSE/DSE, e di verificare chi ha effettuato accessi al proprio FSE/DSE | | | | | |

**Tabella 4 – Misure di dispiegamento**

| 8. | **Requisiti collegati al dispiegamento** | Obbligatoria | Fornitore | | | | **Valutazione Estar** | |
|---|---|---|---|---|---|---|---|---|
| | | | Possibile | | Offerto | | | |
| | | | SI | NO | SI | NO | **Comm.** | **Collaudo** |
| - | Il software consente la gestione aziendale/multi-aziendale con i dati su db criptato | X | | | | | | |
| - | Il software consente la gestione multi-aziendale con separazione fisica dei dati di ciascuna azienda | | | | | | | |
| - | Il software consente la gestione multi-aziendale con separazione logica dei dati di ciascuna azienda | X | | | | | | |
| - | Il livello di Amministratore DBA consente di attribuire separatamente le competenze sulla base anagrafica da quelle sui dati sensibili | | | | | | | |
| - | Il livello di Amministratore DBA consente di attribuire separatamente le competenze sui dati di una Azienda rispetto ai dati di un'altra Azienda gestite nello stesso impianto | | | | | | | |
| - | L'architettura del software, del db e dei servizi utilizzati consente un dispiegamento su due o più nodi in HA in modalità attivo-attivo | | | | | | | |
| - | L'architettura del software, del db e dei servizi utilizzati consente un dispiegamento su due o più nodi in modalità attivo-attivo su LAN geografica | | | | | | | |
| - | È garantita l'indipendenza da figure chiave di amministrazione/gestione, senza le quali non è assicurata l'operatività (ridondanza adeguata delle figure | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| strategiche) | | | | | | | |
| - E’ effettuata la ricerca continua delle vulnerabilità sia sul codice che sulla configurazione | x | | | | | | |

**Tabella 5 – Note esplicative espresse dal Fornitore**

| Note esplicative in relazione alle ipotesi tecniche presentate, con particolare riferimento alle discrepanze tra misure possibili/presenti di più elevata sicurezza e le misure richieste e/o offerte |
|---|
| |

Data compilazione

Il compilatore (Fornitore)