Roma, 18 ottobre 2018

Spett.le AUSL della Romagna
STAFF Direttore Amministrativo
U.O. Governo Sistemi Informativi
c.a. ing. Luigi Santucci
c.a. sig. Stefano Giagnoni

Oggetto: Dichiarazione di conformità ai vincoli normativi del software InterPROfx-InterDELfx di Gestione Protocollo e Delibere a quanto stabilito dal DPCM 3 dicembre 2013 e in tema di misure minime di sicurezza (circ. Agid 2/2017) e compliance alla privacy by design (reg. ue 2016/679)

Gentile Cliente,

con la presente, si dà garanzia che il software InterPROfx-InterDELfx di Gestione Protocollo e Delibere, in uso presso la Vs. Amministrazione, è conforme ai requisiti espressi nel DPCM del 3 dicembre 2013 ed in particolare a quanto specificato negli articoli:

- Art. 9. Formato della segnatura di protocollo;
- Art. 16. Modalità di trasmissione dei documenti informatici mediante l'utilizzo della posta elettronica;
- Art. 18. Modalità di registrazione dei documenti informatici;
- Art. 19. Impronta del documento informatico;
- Art. 19. Impronta del documento informatico.

In tema di sicurezza il prodotto fornisce una serie di strumenti che consentono il pieno rispetto di quanto previsto dal Reg. UE 2016/679 e aderisce;

- ai requisiti riportati nell'articolo 7 del DPCM 3 dicembre 2013;
- alle indicazioni della Circolare Agid n.2/2017 del 18 aprile 2017 in relazione alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

Si precisa inoltre che il software InterPROfx-InterDELfx risulta installato su una infrastruttura hardware che viene gestita direttamente dall'Ente, pertanto i requisiti imposti dalle norme citate che impattano su aspetti organizzativi e sulle modalità di gestione di detti sistemi, non rientrano nelle competenze di Wicome.

Seguono alcune precisazioni tecniche sulla conformità.

Conformità al DPCM 3 dicembre 2013

Modalità di trasmissione e registrazione di documenti informatici

Il sistema non adotta modalità di trasmissione in cooperazione applicativa; lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi di posta elettronica

certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.
Ad ogni messaggio ricevuto o spedito da una area organizzativa omogenea corrisponde un operazione di registrazione di protocollo, secondo quanto previsto dall'art. 53 del testo unico e dall'art. 9 del presente decreto. L'univocità di detta operazione viene garantita da accorgimenti di tipo organizzativo adottati dall'ente, facilitata da alcune funzionalità erogate dall'applicativo atte a verificare che uno stesso messaggio non sia stato già protocollato.
Alla registrazione di protocollo vengono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certifi cata correlati al messaggio oggetto di registrazione.
Il sistema consente la definizione di caselle di posta elettronica certificata e posta elettronica ordinaria, in modo che le stesse possano essere associate alla registrazione di protocollo dei messaggi ricevuti e spediti.

Calcolo dell'impronta dei documenti informatici

Nell'effettuare l'operazione di registrazione di protocollo dei documenti informatici l'impronta di cui all'art. 53, comma 1, lettera f), del testo unico, viene calcolata per ciascun documento informatico associato alla registrazione di protocollo.
La funzione crittografica di hash adottata per la generazione dell'impronta è conforme a quanto stabilito nella deliberazione CNIPA del 21 maggio 2009, n. 45, e successive modificazioni.

Segnatura di protocollo dei documenti

I dati relativi alla segnatura di protocollo di un documento trasmesso dal software Interpro sono associati al documento stesso e contenuti, nel messaggio, in un file, conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale con provvedimento reso disponibile sul proprio sito.
A tal riguardo Wicome garantisce la piena aderenza del software Interpro agli standard, alle modalità di trasmissione, al formato e alle definizioni dei tipi di informazioni scambiate tra le amministrazioni pubbliche e associate ai documenti protocollati stabiliti dall'AgID.
Le informazioni incluse nella segnatura dei documenti trasmessi sono:

a) il codice identificativo dell'amministrazione;
b) il codice identificativo dell'area organizzativa omogenea;
c) il codice identificativo del registro;
d) la data di protocollo secondo il formato individuato in base alle previsioni di cui all'art. 20, comma 2 del DPCM;
e) il progressivo di protocollo secondo il formato specifi cato all'art. 57 del testo unico;
f) l'oggetto;
g) il mittente;
h) il destinatario o i destinatari;
i) l'indice di classificazione;
j) l'identificazione degli allegati.

Compliance alla privecy by design (reg. ue 2016/679)

Sicurezza dei dati (art. 24 e 32 GDPR)

Metodologie di ingegneria informatica utilizzate per lo sviluppo ed il testing

Tutti i processi produttivi (sviluppo, collaudo, manutenzione del software) e di assistenza (monitoraggio e tracciamento delle richieste, del loro stato ed evoluzione) sono eseguiti in osservanza delle procedure operative di Wicome, basate sull'impiego della metodologia di sviluppo software Agile e realizzate in accordo con le best practice in tema di scurezza dei dati e adottando sistemi atti a impedire la vulnerabilità dei codici sorgenti.
L'intero processo di sviluppo agile è caratterizzato da una notevole quantità di test ed utilizzano il modello di sviluppo Test Driven Development (TDD).
L'infrastruttura applicativa del software, garantisce la disponibilità e l'integrità di tutti i dati nel caso in cui si verifichino errori, assicurando l'isolamento e limitando la propagazione delle anomalie nei diversi moduli applicativi.
Il prodotto utilizza un'infrastruttura di persistenza che garantisce l'atomicità delle transazioni effettuate assicurando l'integrità dei dati anche a fronte di errori e situazioni anomale.

Test di vulnerabilità

Il processo di rilascio di ciascuna major release dei prodotti Wicome prevede l'esecuzione di test di vulnerabilità (vulnerability assessment) mediante l'impiego del framework Openvas per l'analisi delle vulnerabilità.
Su richiesta del Cliente Wicome effettua dei test di vulnerabilità sui sistemi in uso presso gli utenti.

Modalità di gestione delle personalizzazioni

Le attività di personalizzazione software di tipo "custom" sono progettate nel rispetto della totale compatibilità e integrazione con la linea di produzione standard, adottando sistemi parametrici con chiavi di attivazione / disattivazione delle funzionalità dedicate.

Soluzioni presenti per la interoperabilità

La soluzione applicativa espone web services che la rendono interoperabile con componenti applicative esterne. Ciascun servizio esposto necessita di una autenticazione che risponde ai requisiti di sicurezza descritti in precedenza e i dati vengono scambiati mediante messaggi SOAP su protocollo cifrato https.

Modalità di manutenzione

La manutenzione del sistema viene eseguita da remoto mediante l'impiego di una VPN. Ciascun operatore abilitato ad accedere al sistema utilizza un'utenza amministrativa ed un certificato di connessione dedicati.

Misure tecniche essenziali

Gestione Utenti e accessi

L'identificazione e l'autenticazione degli utenti vengono effettuate direttamente sul sistema LDAP dell'AUSL. Il prodotto InterproFX - InterdelFX recepisce le seguenti indicazioni previste nella Circolare Agid n.2/2017, con particolare attenzione alle seguenti indicazioni:

1. consente di definire utenze applicative abilitate alle sole funzioni amministrative, registrando ogni accesso effettuato. Sarà cura dell'Ente creare dette utenze, separate dalle utenze applicative abilitate alle altre funzionalità in modo da rispondere in pieno al requisito [ABSC 5.1.2] indicato nella circolare.
2. L'autenticazione viene effettuata dal sistema LDAP gestito dall'Ente e demanda a detto sistema l'aderenza ai requisiti di seguito riportati:
   - ✓ [ABSC 5.7.1] Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri con la regola di avere almeno una maiuscola e un numero)
   - ✓ [ABSC 5.7.3] Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)
   - ✓ [ABSC 5.7.4] Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history)
   - ✓ [ABSC 5.7.2] Impedire che per le utenze amministrative vengano utilizzate credenziali deboli
   - ✓ [ABSC 5.7.5] Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova
   - ✓ [ABSC 5.7.6] Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi

L'autorizzazione viene effettuata dal prodotto sulla base di un sistema di profilazione degli utenti che consente di definire in modo molto granulare ciò che l'utente è in grado di fare e il dominio delle informazioni a cui è abilitato ad accedere.

L'applicazione prevede funzionalità di tipo amministrativo, tali da consentire una profilazione centralizzata e granulare degli utenti.

Cifratura dei dati

Esiste un modulo aggiuntivo dell'applicativo, attivabile a richiesta dell'Ente e dietro rilascio di licenza d'uso, che garantisce la cifratura dei dati e dei documenti registrati.
Gli Enti possono inoltre adottare sistemi di cifratura a protezione delle copie di sicurezza (backup) dei dati ed utilizzare certificati di sicurezza per garantire la cifratura della comunicazione Client-Server.

Gestione dei LOG

Le applicazioni in oggetto prevedono una completa gestione dei log all'interno dell'RDBMS sia per tracciare e registrare le operazioni svolte dagli utenti che accedono all'applicazione tramite le credenziali attribuite, che per tracciare e registrare le operazioni svolte dagli amministratori di sistema che accedono all'applicazione tramite le credenziali attribuite.
Il sistema gestisce la tracciabilità delle modifiche a livello infrastrutturale direttamente sui sistemi RDBMS utilizzati. Il logging avviene a livello applicativo registrando tutte le operazioni previste dal regolamento e quelle critiche a livello di business, anche a livello di lettura dove necessario.
I log prodotti sono consultabili direttamente dall'ambiente applicativo, semplificando così notevolmente le attività degli amministratori di sistema.

Oltre al log applicativo viene prodotto anche il log delle operazioni svolte dal sistema. Per tale tipologia di log è possibile definire il livello di auditing ovvero il livello di dettaglio adottato per tracciare le attività. Queste informazioni vengono memorizzate su file.

Diritti degli interessati (Capo III GDPR)

In relazione alla tipologia del servizio offerto dal modulo software installato, in accordo con l'ente si provvederà a fornire il supporto necessario, implementando misure per fornire assistenza alla committente.

Violazione dei dati (art. 33 e 34 del GDPR)

In relazione alla tipologia del servizio offerto dal modulo software installato, in accordo con l'ente si provvederà a fornire il supporto necessario per adempiere agli obblighi di comunicazione previsti dal GDPR.

Cancellazione dei dati (art. 17 "diritto all'oblio")

In relazione normative specifiche di ogni singolo settore supportato dal software in oggetto Wicome srl fornirà il supporto per rispettare quanto previsto dall'art. 17 del GDPR.

Subfornitori

Nell'esecuzione del contratto non è previsto il coinvolgimento di subfornitori.

Wicome SRL

Firmato digitalmente da

Manuela Quarto

CN = Quarto Manuela
C = IT