Teramo, 25/05/2018

**DICHIARAZIONE DI CONFORMITA SUITE SOFTWARE “TinnVision2030” IN TEMA DI MISURE MINIME DI SICUREZZA (Circ. Agid 2/2017) E COMPLIANCE ALLA PRIVACY BY DESIGN (Reg. UE 2016/679)**

I software della suite “TinnVision2030” di Tinn S.r.l. aderiscono 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)” e garantiscono il pieno rispetto di quanto previsto dal Reg. UE 2016/679.

**Sicurezza dei dati (art. 24 e 32 GDPR)**

L’attenzione per la qualità nella gestione dei vari processi aziendali, che permea tutta l’azienda, è garantita dalla Certificazione del Sistema di Qualità ISO 9001:2015 che Tinn S.r.l. ha conseguito per la progettazione, sviluppo, fornitura e manutenzione di software. Inoltre Tinn S.r.l. ha ottenuto anche la Certificazione del Sistema di Gestione per la Sicurezza delle Informazioni UNI CEI ISO/IEC 27001:2014.

La soluzione proposta, tramite l’infrastruttura applicativa, 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.

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.

La soluzione applicativa è parte di una suite completa che assicura una totale interoperabilità tra i vari moduli che la compongono. La soluzione è inoltre aperta e predisposta all’interazione con altre applicazioni esterne. Il processo di integrazione fra i diversi moduli applicativi (back office e front office) è reso possibile attraverso la definizione di nuove strutture, quali database, flussi di informazioni, estrazione di dati e Web services.

Ove si verificasse la situazione tale per cui parte degli archivi dell’Ente si trovassero in hosting presso il DataCenter, Tinn S.r.l., si impegna a restituire tutti i dati nel loro formato nativo, strutturati e non, al momento della conclusione del contratto (attività di “phase out”).

**Servizio di assistenza e manutenzione**

L’assistenza viene garantita mediante un servizio di help-desk interno alla Tinn S.r.l., per fornire il supporto tecnico-operativo agli utenti dell’Ente interessati alla fruizione dei servizi dell’infrastruttura tecnologica ed applicativa. Il servizio di help-desk eroga le sue attività agli utenti al fine di risolvere le problematiche che si manifestano e per le quali il personale dell’Ente non sia autonomo nella soluzione. Il servizio di help desk viene erogato da personale altamente qualificato, preparato e di comprovata esperienza nel settore della Pubblica Amministrazione Locale ed è in grado di risolvere in modo rapido e puntuale il problema segnalato. Compiti ed attività del servizio di Help desk sono tali da:

* fornire direttamente la soluzione attraverso il canale telefonico, avvalendosi in caso di necessità del supporto del 2° Livello e/o del reparto di Sviluppo software.
* attivare su richiesta del Cliente, previo acquisto di giornate, l’assistenza on-site di personale in modalità affiancamento nel caso di esigenza specifica dell’Ente.

Riguardo ai trattamenti di dati che si dovessero verificare durante le attività di assistenza, a piena tutela del Cliente, si ricorda che i tecnici HelpDesk di Tinn S.r.l.:

* Sottoscrivono accordi di riservatezza per la tutela della protezione dei dati;
* sono tenuti a operare nell'assoluto rispetto della riservatezza di qualsiasi dato o informazione ovvero quant'altro vengano a conoscenza per effetto delle attività svolte ed a non effettuare alcuna attività (copia, estrazione, modifica, cancellazione, etc.) su dati personali salvo il fatto non sia assolutamente necessario a garantire l’integrità o evitare la perdita dei dati e su esplicita richiesta/autorizzazione del cliente che, comunque, avrà sempre il pieno controllo delle attività.

**Misure Tecniche – Gestione Utenti e accessi**

Il sistema di autenticazione degli utenti a TinnVision2030 permette di integrarsi in modo efficace con un sistema di autenticazione LDAP. Il sistema di autenticazione di TinnVision2030 è ovviamente in grado di operare in autonomia anche se non collegato ad un sistema di autenticazione LDAP, in particolare per gestire le situazioni di servizio LDAP momentaneamente offline oppure quando non si voglia proprio fare uso di un LDAP.

L'autenticazione degli utenti è prevista una sola volta, al momento dell'accesso all'applicazione. L'applicazione prevede funzionalità di tipo amministrativo, tali da consentire una profilazione centralizzata e granulare degli utenti.

Nello specifico TinnVision2030 recepisce le seguenti indicazioni previste nella Circolare AgID n.2/2017, con particolare attenzione alle seguenti indicazioni:

* [ABSC 5.1.2] Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato
* [ABSC 5.4.1] Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa
* [ABSC 5.5.1] Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa
* [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 5.7.2] Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
* [ABSC 5.7.3] Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging opzione 30-60- 90 gg)
* [ABSC 5.7.4] Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history opzione 15-20-25 volte)
* [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
* [ABSC 5.10.1] Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministra-tori, alle quali debbono corrispondere credenziali diverse.
* [ABSC 5.10.2] Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconduci-bili ad una sola persona.

**Misure Tecniche – Cifratura dei dati**

Il sistema TinnVision2030 adotta misure di sicurezza a protezione dei dati personali appartenenti alle categorie particolari con la “criptazione dei dati” gestiti dalla suite.

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.

**Misure Tecniche – Log**

La soluzione TinnVision2030 prevede 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 transazionale offrendo il massimo livello di accuratezza e veridicità. Il livello di dettaglio può essere configurato fino ad arrivare alla tracciatura delle letture e non solo delle modifiche. I log prodotti sono consultabili direttamente dall’ambiente applicativo, semplificando così notevolmente le attività degli amministratori di sistema.

**Integrazione con componenti esterne**

Per quanto riguarda l’utilizzo di componenti esterne quali Java e Libre Office, trattandosi di tecnologie e prodotti in continua evoluzione e non potendo avere certezza della retro-compatibilità delle versioni, al fine di garantire la stabilità e il corretto funzionamento dei nostri prodotti, vengono progressivamente certificate le nuove release, previo collaudo dell’intera piattaforma.

**Diritti degli interessati (Capo III Reg UE 679/16)**

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** **Reg UE 679/16)**

In ottemperanza con quanto previsto agli art. 33 e 34 del Reg UE 679/16Tinn S.r.l. rispetterà i tempi di comunicazione previsti dal Reg UE 679/16 o da apposite istruzioni fornite dall’Ente.

Tinn S.r.l.