DICHIARAZIONE DI ADEGUAMENTO SUITE SOFTWARE INAZ
IN TEMA DI MISURE IDONEE DI SICUREZZA E COMPLIANCE ALLA PRIVACY BY DESIGN (Reg. UE 2016/679)

Gentile Cliente,

Con riferimento al quadro normativo in materia di Privacy i software di INAZ Srl sono in continua evoluzione al fine di garantire il pieno rispetto di quanto previsto dal Reg. UE 2016/679 ed in particolare gli sviluppi vengono effettuati nel rispetto dei principi di "privacy by design e privacy by default" definiti dall'articolo 25 del Regolamento UE 2016/679 (GDPR) e tutte le funzioni, gli accorgimenti tecnici e gli strumenti insiti nel software sono stati sviluppati tenendo in considerazione le misure previste dall'art. 32 del GDPR.
In relazione ai trattamenti svolti da Inaz in qualità di responsabile esterno ex art. 28 del GDPR ed effettuati per conto del titolare, gli stessi sono stati descritti nel registro dei trattamenti che individua le soluzioni software utilizzate e le misure di sicurezza ex art 32 del GDPR adottate.

Sicurezza dei dati (art. 24 e 32 GDPR)
Tutti i processi produttivi (analisi, sviluppo, testing, manutenzione del software, collaudo) e di assistenza (monitoraggio e tracciamento delle richieste, del loro stato ed evoluzione) sono eseguiti in osservanza ed in accordo con il Manuale del Sistema di Gestione Integrato di cui alle certificazioni ISO 9001:2015, ISO/IEC 27001:2013 con estensione alle linee guida ISO/IEC 27018:2019, ISO/IEC 27017:2015, ISO/IEC 27035:2016 rilasciate a fronte dell'adozione tra l'altro di sistemi atti a impedire la vulnerabilità dei codici sorgenti.

La soluzione proposta, tramite il framework applicativo, garantisce la riservatezza, la disponibilità e l'integrità di tutti i dati, anche nel caso in cui si verifichino errori, assicurando l'isolamento e limitando la propagazione delle anomalie nei diversi moduli applicativi. I prodotti utilizzano 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.

Le più recenti soluzioni applicative sono parte di una suite completa totalmente integrata ed assicura pertanto una totale interoperabilità tra i vari moduli che la compongono. La soluzione è inoltre aperta e predisposta all'interazione con altre applicazioni esterne, mediante scambio di flussi di dati e/o messaggi utilizzando una tecnologia sicura ed efficiente.

In caso di servizi SaaS erogati dal nostro Datacenter, che hanno ottenuto anche l'accreditamento AGID, INAZ Srl, si impegna a restituire su richiesta tutti i dati nel loro formato nativo, strutturati e non, al momento della conclusione del contratto (attività di dismissione del servizio).

Servizio di assistenza e manutenzione
L'assistenza viene garantita mediante un servizio denominato ATQ o assistenza di sede, in grado di fornire il supporto tecnico-operativo agli utenti dei Clienti. I servizi erogano le loro attività agli utenti al fine di risolvere le problematiche che si manifestano e per le quali il personale del Cliente non sia autonomo nella soluzione. Tali servizi vengono erogati da personale altamente qualificato,

preparato e di comprovata esperienza nel settore HR e sono 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 e/o con collegamento da remoto, avvalendosi in caso di necessitò 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 nel caso di esigenza specifica del Cliente.

Misure Tecniche – Gestione Utenti e accessi

Il sistema di autenticazione degli utenti alle più recenti soluzioni Inaz è in grado di operare in autonomia anche se non collegato ad un sistema di autenticazione 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 i più recenti software di Inaz adottano le seguenti misure (da Inaz definite di livello 1) frutto dell'identificazione di best pratice e di standard di controllo ISO/IEC 27001 ed in particolare:

- Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato
- Utilizzare sia per le utenze amministrative che standard credenziali di elevata robustezza (e.g. almeno 10 caratteri con requisiti di robustezza superiori a quelli previsti in Active Directory)
- Assicurare che le credenziali vengano cambiate con sufficiente frequenza (90 gg con possibilità di riduzione della validità della password) in relazione alla classificazione del dato (es. dati particolari)
- Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history opzione 10 volte di default con possibilità di parametrizzazione)
- Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa
- Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa
- Impedire che per le utenze amministrative vengano utilizzate credenziali deboli
- Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo prima di una nuova modifica
- Controllare che la password non abbiano tutti i caratteri presenti nella Login
- Divieto di utilizzo di password banali
- Controllare la robustezza della prima password
- Cifratura delle password
- Blocco account non utilizzati da più di sei mesi
- Gestione sicura del reset password
- Gestione di gruppi omogenei di utenze a livello di privilegi

Misure Tecniche – Cifratura dei dati (da Inaz definite di livello 2)

Le soluzioni Inaz sono predisposte per l'utilizzo di misure di sicurezza a protezione dei dati particolari mediante cifratura del DB e del file system, su richiesta del Cliente che utilizza il servizio SaaS.
Inaz adotta protocolli sicuri per garantire la riservatezza delle comunicazioni.

Misure Tecniche – Log (da Inaz definite di livello 3)

Le più recenti soluzioni Inaz prevedono, una completa gestione dei log all'interno del DB sia per tracciare e registrare le operazioni svolte dagli utenti che accedono all'applicazione tramite le credenziali assegnate), sia per tracciare e registrare le operazioni svolte dagli amministratori di sistema che accedono alle stesse.
In ambito SaaS, il livello di reportistica dei log può essere configurato tramite un tool esterno di Audit Trail al fine di individuare eventi di sicurezza con livelli diversi di rilevanza. I log prodotti sono consultabili direttamente dall'ambiente applicativo, semplificando così notevolmente le attività degli amministratori di sistema.

Diritti degli interessati (Capo III GDPR)
In relazione alla tipologia del servizio offerto dal modulo software installato, su richiesta del Cliente si provvederà a fornire il supporto necessario, implementando misure per fornire assistenza al committente.
Inoltre sono stati implementati nei software specifici menù e processi semiautomatici per la gestione delle richieste degli interessati ed in particolare:

- Diritto alla Portabilità
  E' stato predisposto un report con i dati personali che il candidato o la risorsa ha comunicato. I dati che vengono estratti saranno principalmente dai Anagrafici (residenza, domicilio, dati del conto corrente) familiari a carico e dati fiscali ove presenti. Tale estrazione è parametrizzabile da parte del cliente oppure tramite intervento da parte di un consulente Tecnico.

- Diritto all'oblio (cancellazione)
  Tramite una funzione di mascheramento dei dati relativi ai candidati esterni. Questa funzione è distribuita con un set standard di campi (che potranno essere variati ma solo con richiesta di personalizzazione) e con un avviso che comunichi chiaramente all'utente che in caso di esecuzione non sarà possibile recuperare i dati del candidato. Tale operazione dovrà essere eseguita solo dopo l'eventuale estrazione dei dati nel caso l'utente li richieda prima di esercitare il diritto all'oblio. Il Diritto all'oblio non potrà essere applicato in caso di dati personali da conservare a fini fiscali/previdenziali.

- Per il Diritto di Rettifica ed il Diritto di Limitazione del Trattamento dei Dati è stato creato uno specifico Registro nel quale, all'atto della richiesta da parte dell'interessato verrà inserita la data, il tipo di richiesta, il richiedente e i dati coinvolti, per poter tracciare la modifica e conseguentemente la data di chiusura/revoca. Le richieste da parte degli interessati verranno evidenziate agli autorizzati al trattamento tramite opportuno "Widget" al fine di adottare le necessarie misure (es. comunicazioni da parte dell'Ufficio del personale) in relazione alle tipologie di richieste e alla conseguente applicabilità ai dati oggetto di trattamento.

Inaz è disponibile allo sviluppo di personalizzazioni a fronte di specifiche esigenze che verranno vagliate di fattibilità.

Violazione dei dati (art. 33 e 34 del GDPR)
In ottemperanza con quanto previsto agli art. 33 e 34 INAZ Srl rispetterà per i servizi SaaS i tempi di comunicazione previsti dal GDPR mentre per le soluzioni in house il Cliente dovrà richiedere uno specifico intervento di assistenza.

Milano, 02 marzo 2021

Inaz S.r.l Soc. Unip.