Misure tecniche e organizzative applicate dalle SWH per garantire i requisiti di Privacy by Design e by Default nelle Attività di sviluppo dei Software Gestionali

Nel presente Allegato tecnico sono definite le misure tecniche e organizzative che, sin dalla progettazione e per impostazione predefinita, il SW deve prevedere per consentire l'attuazione efficace dei principi di protezione dei dati e l'integrazione delle adeguate garanzie per l'osservanza dei requisiti previsti dal GDPR da parte dei Clienti che tratteranno dati personali mediante l'impiego dei SW prodotti dalle imprese aderenti al suddetto Codice di condotta.

In linea con il Considerando 78 e l'art. 25 del GDPR, i requisiti e gli standard indicati nel presente Allegato sono stati definiti tenendo conto anche delle "Linee guida 4/2019 sull'articolo 2. Protezione dei dati fin dalla progettazione e per impostazione predefinita Versione 2.0" (LG4/2019), nonché considerando le misure, applicabili allo sviluppo del software, di seguito elencate come elementi fondamentali per il rispetto dei principi di "integrità e riservatezza" (paragrafo 3.8 di tali Linee guida).

Le misure sono state anche confrontate, laddove applicabili allo sviluppo del software con:

1. i controlli presenti nella "UNI CEI ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements " (ISO/IEC 27002:2022);

2. i controlli per la "Privacy in base alla progettazione e privacy per impostazione predefinita" elencati nel paragrafo A.7.4 della "ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines" (ISO/IEC 27701:2019);

3. le misure comprese nelle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" emanate dall'AgID (MM AgID);

4. le misure elencate riguardanti la "Sicurezza delle informazioni" presenti nel paragrafo 5.11 di " Information technology - Security techniques - Privacy framework" (ISO/IEC 29100:2011).

Le misure di sicurezza sono state inoltre associate ai parametri RID (riservatezza, integrità e disponibilità) utili per una valutazione degli impatti per gli interessati.

Ambito	**Catalogazione**	**Requisito di dettaglio**	**Riferimenti**	**RID**
Principi di sviluppo del SW Gestionale	Analisi di nuove funzioni	Valutazione e documentazione nelle analisi delle funzioni applicative del rispetto dei principi di minimizzazione: - nel dato: ogni dato personale raccolto dal SW deve essere necessario rispetto alla finalità della raccolta - nell'uso: ogni dato personale deve essere trattato solo da coloro che ne abbiano un'effettiva necessità - nel tempo: il dato personale deve essere trattato per il tempo strettamente necessario per il perseguimento della finalità. In particolare, già in fase di analisi devono essere identificati i dati personali trattati, la durata prevista dal trattamento, l'indicazione dei ruoli che vi potranno accedere, l'indicazione dei processi che vi potranno accedere, l'indicazione degli output.	ISO/IEC 27701:2019 A.7.4.4	RID

Definizione della protezione dell'accesso ai dati	Documentazione degli strumenti e dei requisiti per l'utilizzo del SW	Documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.). Documentazione dei sistemi operativi e dei requisiti per l'utilizzo del SW.	ISO/IEC 27701:2019 A.7.4.2, A.7.4.4	
Autenticazione	Modalità e regole di autenticazione	Utilizzo di utenze nominative individuali al fine di garantire la tracciabilità delle operazioni eseguite. Conformità della password policy alle best-practice europee e internazionali di riferimento che ne garantiscano sicurezza adeguata, sia in termini di complessità (es. minimo 8 caratteri presenza di caratteri speciali, maiuscole, etc.), scadenza (durata fissa o modulabile dal cliente/titolare del trattamento), ciclicità della password (es. non consentire il riuso di password precedenti), gestione reset delle password con sistemi che garantiscano l'identificazione del richiedente e simili. Adozione di misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from	ISO/IEC 27002:2022 5.15,5.16, 5.17, 5.18 MM AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RI

		the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against a large number of different accounts).	
		MF Authentication	MFA (quali ad es. OTP, smartcard ecc.) implementabili in base al livello di rischiosità dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento. Tra i fattori di autenticazione prevedere anche la possibilità di autenticare anche il singolo device che si collega in relazione alla rischiosità del trattamento.
		Gestione accessi	Adozione di misure che consentono di monitorare e gestire i rischi inerenti agli accessi ai sistemi applicativi, tra cui, a titolo esemplificativo: - disattivazione delle credenziali in caso di inutilizzo per tempi prolungati (es.: sei mesi); - disattivazione temporanea o definitiva in caso di superamento di un numero impostato di tentativi di accesso falliti reiterati;

		- impostazione di time out della sessione attiva; - visualizzazione data e ora ultimi accessi; - salvataggio dei log di accesso al sistema in modo che i clienti possano esportali a sistemi terzi di conservazione che ne garantiscano l'integrità e la conservazione per i tempi definiti dai clienti stessi.		
	API	Adozione di misure di autenticazione per le API (es.: certificato digitale; token, ecc.).		
Profili di accesso	Profili di accesso	Gestione delle utenze, sia utilizzate dal cliente per effettuare attività di amministratori del sistema (ad esempio per essere autonomi nella generazione delle utenze o nell'impostare parametri di utilizzo), sia per l'utilizzo del sistema stesso, in conformità a procedure volte a garantire il rispetto del principio di minimo privilegio e un'adeguata segregazione dei compiti gli utenti devono accedere solo a funzioni, file di dati, URL, controller, servizi e altre risorse, per le quali possiedono un'autorizzazione specifica. Le eventuali utenze generate per far accedere gli incaricati del trattamento del fornitore al fine di prestare assistenza sul prodotto utilizzato saranno identificate nominalmente e avranno profilo di accesso amministrativo e saranno gestite dal cliente con relativa attivazione	ISO/IEC 27002:2022 5.3, 5.1.5, 5.1.6, 5.1.8 MM AgID ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 ISO/IEC 29100:2011 5.11	R

		e disattivazione in caso di necessità di utilizzo.		
Autenticazione	Gestione delle autorizzazioni	Inventario delle utenze presenti nel sistema con i relativi profili di autorizzazione assegnati, disponibile al cliente per sua rendicontazione e analisi degli accessi.	ISO/IEC 27002:2022 5.3, 5.1.5, 5.1.6, 5.1.8 MM AgID ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 ISO/IEC 29100:2011 5.11	R
Protezione archivi dati Cliente	Protezione dati Cliente	Adozione di tecniche di pseudonimizzazione o cifratura dei dati (tokenizzazione, etc.) adottabili dal Cliente ove appropriate allo scopo di garantire un adeguato livello di protezione in relazione alle tipologie di dati personali trattati (es.: categorie particolari ex art. 9 del GDPR e dati penali ex art. 10).	ISO/IEC 27002:2022 5.10 MM AgID ABSC 13.3.1 ISO/IEC 29100:2011 5.11	RI

Protezione archivi	Protezione archivi contenenti le password	Adozione, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines).	ISO/IEC 27002:2022 8.24	RI
Sicurezza SW	Secure coding	Adozione di policy e procedure finalizzate a garantire che lo sviluppo degli applicativi avvenga nel rispetto di linee guida di secure coding conformi alle best practices (quali, ad es., OWASP, controllo delle librerie di terze parti costante e identificazione di eventuali criticità con segnalazione ai clienti e sostituzione immediata delle librerie che comportano criticità nel trattamento dei dati, etc.).	ISO/IEC 27002:2022 8.25	RI
	Minacce e Vulnerabilità	Test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), se il SW è destinato ad essere esposto su reti pubbliche Adozione di un piano di miglioramento che analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione.	ISO/IEC 27002:2022 8.8 MM AgID ABSC MM AgID ABSC 4.1.1, 4.1.2, 4.4.2, 4.6.1 ISO/IEC 29100:2011 5.11	RID

		Svolgimento periodico di analisi di vulnerabilità.	ISO/IEC 27002:2022 8.8 MM AgID ABSC MM AgID ABSC 4.1.1, 4.1.2, 4.4.2, 4.6.1 ISO/IEC 29100:2011 5.11	RID
	Log applicativi di attività utente	Funzionalità per il tracciamento del log degli accessi e delle attività svolte in relazione alle diverse tipologie di utenza (amministratore, super utente, utente, etc.) allo scopo di consentire al titolare o al responsabile del trattamento un'adeguata attività di monitoraggio. I log riguardanti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore del sistema del Cliente.	ISO/IEC 27002:2022 8.15 MM AgID ABSC 5.4.1, 5.1.1	RID
Requisiti sistemistici e di gestione				

Ambienti di test	Misure per ambienti di test	Separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e previsione di misure di accesso mediante credenziali e privilegi diversi in modo di ridurre al minimo i rischi.	ISO/IEC 27002:2022 8.31, 8.33 MM AgID ABSC 4.10.1, 8.2.3	RI

Funzioni specifiche	Data retention	Previsione di funzioni del SW che consentano ai clienti di impostare la cancellazione dei dati personali trascorso il periodo necessario di loro conservazione. Il SW deve prevedere estrazioni di dati che consentano ai clienti di essere consapevoli sui periodi di conservazione dei dati al fine di trattare i dati secondo il principio di minimizzazione.	ISO/IEC 27701:2019 A.7.4.7	RID

Funzioni specifiche	Portabilità	Funzionalità idonee a consentire al Cliente l'estrazione dei dati personali in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo in caso di esercizio del diritto alla portabilità da parte dell'interessato, ove ne ricorrano i presupposti.	GDPR art. 20	D
Misure organizzative	Formazione	Erogazione periodica alle persone autorizzate al trattamento di corsi di formazione sulla sicurezza e protezione dei dati personali. Per gli sviluppatori sono previsti anche corsi di sviluppo sicuro.	ISO/IEC 27002:2022 6.3 MM AgID ABSC 8.7.2, 8.7.3, 8.7.4	RID
Misure di sicurezza	Backup	Funzionalità al fine di permettere al Cliente di effettuare, anche tramite processi esterni, il salvataggio o backup dei dati trattati dall'applicativo.	ISO/IEC 27002:2022 8.13 MM AgID ABSC 10.1.2 ISO/IEC 29100:2011 5.11	ID

Misure di sicurezza	Esattezza e accuratezza dei dati	Adozione di misure per assicurare al Cliente una verifica dell'esattezza e dell'accuratezza dei dati (ad es. controlli di correttezza formale della PIVA o CF).	ISO/IEC 27701 A.7.4.3	RI

Misure di sicurezza	Riservatezza dei dati		Adozione di misure per agevolare il Cliente nel rispetto del requisito della riservatezza in caso di utilizzo di funzioni di condivisione dei dati (tramite ad es. l'invio di avvisi o notifiche).	ISO/IEC 27701 A.7.4.3	R
Misure organizzative	Inventory Librerie		Conservazione dell'inventario delle componenti software in uso comprensive delle librerie di terzi e/o open source in modo da poter rispondere più tempestivamente in caso di segnalazioni di vulnerabilità (SBOM SW bill of materials).	ISO/IEC 27002:2022 5.6, 8.4 MM AgID ABSC 2.1.1	RID

Misure organizzative	Change management	Regolamentazione del processo di gestione delle modifiche applicative ed infrastrutturali, al fine di garantire un miglior presidio di ogni fase del ciclo di vita del SW e di tracciarne l'evoluzione, con monitoraggio dei livelli di accesso alle informazioni critiche e adeguata formazione/sensibilizzazione delle persone coinvolte nel processo di Change Management (al rispetto dei principi di *Segregation of Duties*).	ISO/IEC 27002:2022 5.3, 8.32	D
Misure organizzative	Configuration management	Regolamentazione del processo di Configuration management al fine di garantire la corretta gestione delle versioni dei rilasci dei moduli SW.	ISO/IEC 27002:2022 8.9	RID
Misure di sicurezza	Trasmissione dati personali	Utilizzo di protocolli sicuri e adeguati allo sviluppo tecnologico per proteggere i dati durante la loro trasmissione.	ISO/IEC 27002:2022 5.10, 5.14, 8.26 ISO/IEC 27701:2019 A.7.4.9 Misure Minime AgID ABSC 3.3.2 ISO/IEC 29100:2011 5.11	RI

Misure di sicurezza	File temporanei	Funzionalità per permettere l'eliminazione dei file temporanei contenenti dati personali e creati durante i trattamenti e cancellazione sicura dei dati sugli strumenti dismessi (*Secure disposal*).	ISO/ISO 27701: A.7.4.6	R