CODICE DI CONDOTTA PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO DALLE IMPRESE DI SVILUPPO E PRODUZIONE DI SOFTWARE GESTIONALE

(Pubblicato sulla Gazzetta Ufficiale Serie Generale del 278 del 27 novembre 2024)

VEDI ANCHE PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI N. 618 DEL 17 OTTOBRE 2024

INDICE

- Articolo 18 – Cooperazione con le Autorità di controllo, con l'Autorità giudiziaria e di polizia giudiziaria e tributaria
- Articolo 19 – Verifiche sul rispetto del Codice di condotta ed organismo di monitoraggio
- Articolo 20 – Modalità di adesione al Codice di condotta
- Articolo 21 – Riesame del Codice di condotta
- Articolo 22 – Entrata in vigore del Codice di condotta

Allegati:

- Allegato A: 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
- Allegato B: Misure di sicurezza applicate dalle SWH per lo svolgimento dei Servizi riguardanti i SW Gestionali impiegati nei contesti on premise e in cloud
- Allegato C: Schema di accordo sul trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679- Regolamento Generale sulla Protezione dei Dati
- Allegato D: Organismo di Monitoraggio
- Allegato E: Modalità di adesione al Codice di condotta

PREAMBOLO

Le imprese produttrici del Software Gestionale aderenti ad Assosoftware hanno promosso l'adozione del presente Codice di condotta sulla base di quanto previsto dall´art. 40 del Regolamento (UE) n. 679/2016 - Regolamento Generale sulla Protezione dei Dati (di seguito denominato "**Regolamento**" o "**GDPR**"), in considerazione delle seguenti premesse.

1. Assosoftware è l'associazione italiana che riunisce, rappresenta e tutela le principali aziende produttrici di Software Gestionale per piccole e medie imprese, professionisti e pubbliche amministrazioni. Il settore del Software Gestionale costituisce un fattore chiave per la crescita delle competenze digitali e la modernizzazione dei processi produttivi, elementi fondamentali per la competitività degli operatori a livello internazionale o globale, e per lo sviluppo del sistema Paese, sia per il suo impatto diretto su economia ed occupazione, sia per l'indotto generato in termini di digitalizzazione di imprese, professionisti e pubbliche amministrazioni lungo tutta la catena del valore, dal front-end verso i clienti e cittadini, al back end di produzione, fino alla gestione documentale e amministrativa.

2. In questo contesto, emerge la concreta esigenza per le imprese produttrici rappresentate da Assosoftware di assicurare che le attività dalle stesse svolte nell'ambito dell'intero ciclo di vita del software gestionale, dalla sua progettazione, produzione e sviluppo sino alla sua installazione e messa in esercizio, si conformino ad elevati livelli di protezione dei dati personali, allo scopo di favorire il rispetto del Regolamento e di rafforzare la fiducia degli utilizzatori del software verso l'adozione dei soluzioni gestionali in grado di realizzare la transizione digitale e l'innovazione produttiva. Il software gestionale, infatti, consente l'automazione dei principali processi interni di imprese (es. processi di approvvigionamento, gestione del magazzino, vendite, fatturazione, rapporti con i clienti, gestione documentale etc.), di professionisti (es. software per la gestione dello studio professionale, delle attività contabilità, tributarie, lavoristiche, legali e fiscali) e delle Pubbliche Amministrazioni (es. processi di e-procurement, gestione delle gare e commesse, etc.), con un evidente e notevole impatto sugli aspetti relativi alla protezione dei dati personali. In tal senso, si pone, altresì, la ulteriore esigenza di fornire strumenti adeguati di digitalizzazione, anche per favorire la conformità degli operatori più piccoli del mercato, che, a livello tecnico e informatico, potrebbero difettare delle risorse o competenze necessarie, e per contemperare le esigenze di semplificazione degli adempimenti delle PMI e dei professionisti con la necessità di garantire un'elevata tutela dei diritti degli interessati.

3. Per i motivi sopra esposti, le imprese produttrici del software gestionale (c.d. "**Produttori del Software**" o "***Software House*** *–* ***SWH***"), associate ad Assosoftware, hanno promosso ed avviato l'elaborazione di un progetto di Codice di condotta ai sensi del citato art. 40 del GDPR, diretto a fornire un concreto ed effettivo contributo alla definizione degli impegni assunti per garantire il diritto alla protezione dei dati personali in fase di progettazione e sviluppo di applicazioni, servizi e prodotti software, in considerazione dell'evoluzione tecnologica e dei relativi costi di attuazione, con l'obiet-

tivo di rendere disponibili ai Clienti, operanti quali Titolari o Responsabili del trattamento, idonei strumenti e funzionalità per adempiere ai loro obblighi di protezione dei dati in relazione ai trattamenti svolti tramite i predetti software

4. In particolare, i Produttori del Software intendono attraverso il presente Codice definire un sistema uniforme ed avanzato di regole di condotta e misure tecniche e organizzative, per assicurare che i software prodotti e resi disponibili sul mercato siano sviluppati nel rispetto dei principi di protezione dei dati fin dalla progettazione (*by design*) e per impostazione predefinita (*by default*), al fine di dimostrare la conformità alle disposizioni del Regolamento e di rafforzare la fiducia verso la digitalizzazione dei servizi e processi degli operatori economici ed istituzionali che li utilizzano, assicurando un adeguato livello di tutela dei dati personali trattati tramite l'impiego dei medesimi software.

5. L'adozione del presente Codice di condotta e l'adesione da parte delle SWH per uno o più prodotti dagli stessi sviluppati sono volte quindi a promuovere tra i Clienti richiedenti ed utilizzatori di Software Gestionali:

i. la conformità by design/default di tali Software al Regolamento ed alla normativa nazionale applicabile in materia di protezione dei dati (v., in particolare, il d.lgs. n. 196/2003 e s.m.i, recante il Codice in materia di protezione dei dati personali);

ii. l'adeguatezza delle misure tecniche e organizzative offerte dai Produttori in relazione all'intero ciclo di vita dei Software sviluppati, ove impiegati per attività di trattamento di dati personali.

6. Il presente Codice ha ad oggetto non solo le attività di progettazione e sviluppo dei Software, che di regola non comportano il trattamento di dati personali, ma anche le attività di installazione, test, collaudo, assistenza, manutenzione e aggiornamento dei Software Gestionali, che possono comportare operazioni di trattamento di dati personali eseguite dai Produttori per conto dei Clienti, (es.: attività di migrazione dati finalizzata all'installazione del Software, attività di assistenza e aggiornamento SW con accesso da remoto, acquisizione o esportazione di copia di dati per verifica di problematiche tecniche, ecc.). Queste ultime attività possono essere svolte in diversi contesti: (i) ***on premise***, ossia quando il Software è installato su infrastrutture, apparati e sistemi del Cliente (o di fornitori di quest'ultimo), e (ii) ***cloud,*** laddove il Cliente utilizzi il Software del Produttore attraverso infrastrutture rese disponibili da quest'ultimo (direttamente o tramite suoi sub-fornitori).

7. In linea con le premesse e gli obiettivi su esposti, i Produttori del Software Gestionale si limitano solo a sviluppare e a mettere a disposizione del Cliente prodotti Software per la gestione dei processi organizzativi strumentali ai servizi di elaborazione dati il cui trattamento rientra nella sfera di responsabilità del Cliente, quale Titolare del trattamento o Responsabile. Il presente Codice di condotta non ha ad oggetto e non intende pertanto disciplinare le attività di trattamento di dati personali even-

tualmente svolte dal Produttore del Software, su richiesta e per conto del Cliente, quali servizi di elaborazione di dati a fini contabili, amministrativi, retributivi, previdenziali, assistenziali e fiscali (es. elaborazione paghe, tenuta della contabilità, fatturazione, ecc.).

Articolo 1 - Ambito di applicazione

1.1. Il presente Codice di condotta è riferito alle attività di trattamento di dati personali poste in essere dai Produttori del Software nei contesti di cui in premessa, limitatamente al territorio dello Stato Italiano ed è applicabile unicamente a livello nazionale. Per tale motivo, l'approvazione di cui all'art. 40 del Regolamento è richiesta al Garante in qualità di Autorità di controllo competente ai sensi dell'art. 55 del Regolamento.

1.2. Il presente Codice di condotta è applicabile nei confronti di ciascun Software Gestionale, per il quale il Produttore presenti richiesta di adesione ai sensi del successivo art. 20.

1.3. Il presente Codice di condotta non è applicabile nei riguardi dei trattamenti di dati personali connessi allo svolgimento da parte della Software House di attività secondarie o comunque non riguardanti la produzione del Software Gestionale, che sono comuni e traversali rispetto alla generalità dei settori produttivi (come, ad es., il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, il trattamento di dati personali dei Clienti, anche potenziali, a fini di marketing diretto, ecc.).

Articolo 2 – Definizioni

2.1. Ai fini del presente Codice di condotta, si applicano le definizioni previste dall'art. 4 del Regolamento.

2.2. Ai medesimi fini, si intende per:

a) Produttori del Software (anche Produttore, *Software House* o *SWH*): le imprese che progettano, sviluppano e producono Software Gestionali;

b) Software Gestionale: i programmi di elaborazione elettronica che consentono ad aziende, professionisti e pubbliche amministrazioni di automatizzare, informatizzandoli, i processi di organizzazione e gestione delle rispettive attività;

c) Servizi: i servizi relativi alle attività di installazione, messa in esercizio, assistenza, manutenzione, gestione, aggiornamento del Software Gestionale prodotto dalla SWH;

d) Attività di Sviluppo: le attività di progettazione, sviluppo e produzione del Software Gestionale, che non comportano di regola lo svolgimento di attività di trattamento di dati personali;

e) Clienti: i soggetti che richiedono ai Produttori lo sviluppo ed installazione dei Software Gestionali e le connesse attività di manutenzione ed assistenza, sottoscrivendo i relativi contratti od accordi di licenza e utilizzo;

f) Utenti: le persone fisiche (quali, ad es., rappresentanti, esponenti, dipendenti e collaboratori) autorizzate (i) dal Cliente ad accedere ed utilizzare per suo conto il Software e i relativi Servizi, e/o (ii) dal Produttore del Software a svolgere i Servizi;

g) Accordo sul trattamento dei dati personali: l'accordo scritto sul trattamento dei dati personali sottoscritto dal Produttore del Software e dal Cliente ai sensi dell'art. 28 del Regolamento per lo svolgimento dei Servizi;

h) Garante: il Garante per la protezione dei dati personali di cui agli artt. 2-bis e 153 del d.lgs. n. 196/2003 – Codice in materia di protezione dei dati personali, e successive modificazioni ed integrazioni.

Articolo 3 - Progettazione e sviluppo di SW Gestionali: Privacy by Design e by Default

3.1. Le Attività di Sviluppo dei Software Gestionali sono improntate al rispetto dei principi di protezione dei dati sin dalla progettazione e per impostazione predefinita, di cui all'art. 25 del Regolamento, e vengono documentate dai Produttori del Software attraverso:

i) la valutazione dei rischi dei trattamenti dei dati personali cui il Software Gestionale è preordinato;

ii) la previsione di funzionalità, misure tecniche e organizzative che consentano al Cliente, quale Titolare o Responsabile del trattamento, di garantire un adeguato livello di protezione ai dati personali trattati attraverso il Software Gestionale;

iii) la comunicazione in modo trasparente al Cliente delle caratteristiche di sicurezza e di privacy by design del Software Gestionale, in modo che possa valutare sotto la propria responsabilità se, sul piano tecnico, il medesimo Software è conforme alle proprie esigenze e alle caratteristiche specifiche del trattamento di dati personali che intende effettuare tramite lo stesso. Ove il Cliente ritenga necessarie misure aggiuntive, il Produttore del Software può valutarne la fattibilità tecnica e gli oneri associati.

3.2. Nella progettazione e sviluppo dei Software Gestionali, i Produttori si attengono alle misure indicate nell'Allegato A del presente Codice al fine di:

- assicurare un adeguato livello di protezione dei dati personali trattati tramite il Software Gestionale;

- offrire le idonee garanzie richieste, a livello tecnico e di sicurezza, dal Regolamento;

- facilitare, anche attraverso il riferimento alle corrispondenti disposizioni del Regolamento e delle norme internazionali pertinenti, i Clienti, gli Interessati, l'OdM e il Garante nelle valutazioni sulla conformità del Software ai requisiti del presente Codice.

3.3. L'Allegato A è riesaminato e aggiornato periodicamente, anche sulla base dell'evoluzione dello sviluppo tecnologico e degli scenari di rischio.

3.4. Le misure previste nell'Allegato A dovranno essere implementate nell'ambito delle Attività di Sviluppo delle soluzioni di Software Gestionali, per le quali viene presentata dai Produttori domanda di adesione al presente Codice ai sensi del successivo articolo 20.

Articolo 4 - Installazione, assistenza e manutenzione del SW Gestionale

4.1. In relazione allo svolgimento delle attività tecniche relative ai Servizi nei contesti on premise e in cloud, che possono comportare operazioni di trattamento di dati personali per conto del Cliente, il Produttore del Software assume il ruolo e gli obblighi di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento, e si conforma a quanto indicato ai successivi articoli 5 e 6. In questi casi, laddove il Cliente (come nel caso, ad es., di professionisti) sia Responsabile del trattamento, la SWH rivestirà il ruolo di ulteriore Responsabile (c.d. "**Sub-Responsabile**") di tale trattamento ai sensi del citato art. 28, paragrafi 2 e 4.

4.2. In particolare, il Produttore del Software opera quale Responsabile o Sub-Responsabile del trattamento nei contesti relativi alla esecuzione dei Servizi in cloud, mentre, nei contesti on premise, può rivestire tale ruolo solo qualora venga chiamato a svolgere attività tecniche connesse alla installazione, assistenza e manutenzione del Software Gestionale che possano comportare un trattamento di dati personali, come, per esempio, nel caso di:

a) attività di migrazione dati finalizzata all'installazione e al collaudo del Software Gestionale;

b) attività di assistenza e aggiornamento del Software Gestionale con possibilità (ancorché occasionalmente) di accesso remoto ai dati del cliente (es. tramite strumenti di help-desk remoto VPN, ecc.);

c) attività di acquisizione di data base del Cliente o esportazione e copia di dati personali del Cliente per verificare problematiche di carattere tecnico e svolgere attività di assistenza e manutenzione.

4.3. Nei contesti on premise e in cloud, fermo il rispetto delle misure di cui al precedente art. 3 e all'Allegato A, il Produttore del Software, quale Responsabile o Sub-Responsabile del tratta-

mento, si impegna ad osservare le misure di sicurezza di cui all'Allegato B del presente Codice di condotta.

4.4. Resta fermo che, nei contesti on premise:

i) al personale incaricato dal Produttore del Software, che svolge in via continuativa attività di assistenza e manutenzione che comporta l'accesso ad infrastrutture e sistemi del Cliente su cui è installato il medesimo Software, sono attribuite le funzioni di amministratore di sistema, nel rispetto del provvedimento del Garante recante misure e accorgimenti in materia di amministratori di sistema, fermo quanto previsto al successivo art. 11.4;

ii) le attività e gli obblighi del Produttore quale Responsabile del trattamento non si estendono alle attività di gestione e manutenzione dell'infrastruttura su cui è installato il Software Gestionale, la cui responsabilità resta a carico del Cliente. In particolare, restano escluse, nei contesti on premise, dalla responsabilità del Produttore del Software, le attività di salvataggio e ripristino dei dati personali così come tutte le attività necessarie alla protezione della sicurezza fisica e logica dell'infrastruttura su cui il Software è installato.

Articolo 5 - Ruolo della SWH quale Responsabile del trattamento: garanzie, obblighi e responsabilità

5.1. Attraverso l'adesione al presente Codice e l'adozione delle misure di cui all'Allegato A e all'Allegato B, il Produttore del Software assicura l'adeguatezza delle garanzie prestate quale Responsabile o Sub-Responsabile del trattamento, ai sensi dell'art. 28, par. 1, del Regolamento, ferma restando la possibilità di integrare eventualmente tali garanzie anche tramite l'adesione ad ulteriori codici di condotta, ove applicabili, oppure certificazioni o l'adesione a best practice di settore (quali, ad es., le norme ISO).

5.2. Non rientra tra gli obblighi a carico del Produttore del Software la determinazione dei presupposti di liceità delle attività di trattamento dei dati svolte per conto del Cliente. Resta ferma la possibilità per il Produttore del Software di rifiutarsi di eseguire attività di trattamento dei dati che risultino palesemente in contrasto con la vigente normativa in materia di protezione dei dati personali, dandone evidenza al Cliente.

Articolo 6 - Accordo sul trattamento dei dati personali con il Cliente

6.1. Nei casi previsti ai precedenti artt. 4 e 5, il Produttore del Software stipula con il Cliente, anche in forma elettronica, un Accordo sul trattamento dei dati personali ai sensi dell'art. 28 del Regolamento e in osservanza delle Linee guida del Comitato Europeo per la Protezione dei Dati

("EDPB") attualmente applicabili a tale riguardo (cfr. Linee Guida n. 7/2020). L'Allegato C al presente Codice riporta uno schema meramente esemplificativo e non vincolante dei principali contenuti dell'Accordo sul trattamento dei dati personali, elaborato sulla base delle linee guida dell'EDPB, al fine di agevolare i Produttori del Software aderenti al presente Codice, soprattutto ove si tratti di PMI, nell'adempimento di tali obblighi. Le disposizioni dell'Accordo sul trattamento dei dati personali ex art. 28 del Regolamento non possono in alcun modo derogare a quanto previsto nel presente Codice.

6.2. Laddove i Servizi siano erogati ad un elevato numero di Clienti, il Produttore del Software può proporre un proprio schema di Accordo ex art. 28, contenente tutti gli elementi di cui all'art. 28.3 e avente condizioni contrattuali uniformi e indicazione delle misure tecniche e organizzative garantite, che permetta un'omogenea ed efficace gestione degli obblighi assunti.

6.3. I precedenti commi si applicano anche nel caso in cui il Cliente dichiari di agire quale Responsabile del trattamento ai sensi del precedente art. 4 e di avvalersi del Produttore del Software quale ulteriore Responsabile del trattamento.

Articolo 7 – Ricorso della SWH a Sub-Responsabili del trattamento

7.1. Ai fini del presente articolo, si configura quale "Sub-Responsabile" del trattamento il soggetto esterno (persona fisica o giuridica), a cui sono affidati dalla SWH Servizi che comportano un trattamento di dati personali effettuato dal medesimo Produttore quale Responsabile o Sub-Responsabile per conto del Cliente e che abbiano un rapporto di diretta dipendenza funzionale rispetto ai servizi o attività oggetto del contratto in essere tra il Produttore del Software ed il medesimo Cliente, quale Titolare del trattamento.

7.2. In caso di rilascio da parte del Cliente, all'interno dell'Accordo sul trattamento dei dati ai sensi dell'art. 28 del Regolamento, di un'autorizzazione scritta generale alla nomina di "Sub-Responsabili", questa deve essere riferita a categorie di Sub-Responsabili, individuate anche per tipologia di servizio reso, e rinviate ad un elenco nominativo (da fornire su richiesta del Titolare e da rendere disponibile a quest'ultimo attraverso modalità che ne permettano l'agevole consultazione). Il Produttore del Software può modificare o integrare l'elenco dei Sub-Responsabili dandone comunicazione al Cliente, ove possibile con congruo preavviso, attraverso le modalità anche semplificate concordate con il Cliente, quali, ad esempio, un'area riservata o utilizzando i canali di comunicazione previsti contrattualmente. Il Produttore del Software non può ricorrere ad ulteriori Responsabili senza la preventiva autorizzazione del Cliente.

7.3. Coerentemente con quanto concordato nell'Accordo per la protezione dei dati personali, il Produttore del Software deve prevedere che il Cliente possa opporsi alla individuazione di uno o più Sub-Responsabili entro trenta (30) giorni dal ricevimento della comunicazione, esprimendo le motivazioni poste a corredo della propria opposizione. Laddove non sia possibile addivenire ad una soluzione condivisa, il Cliente può recedere dal contratto relativo al Software Gestionale utilizzato, nei termini dallo stesso previsti.

7.4. Il Produttore del Software si impegna a mantenere un elenco aggiornato dei Sub-Responsabili coinvolti nel trattamento dei dati del Cliente, nel quale siano indicati nominativo o denominazione legale, sintetica descrizione del trattamento affidato e luogo del trattamento, ove svolto al di fuori del territorio nazionale od europeo, e si impegna a renderlo disponibile, su richiesta del Cliente. Per la fornitura della lista degli ulteriori Sub-Responsabili coinvolti, il Produttore del Software può richiedere la sottoscrizione di idonei impegni di riservatezza.

7.5. Il Produttore del Software si impegna a sottoscrivere con ogni Sub-Responsabile un accordo sul trattamento dei dati personali, il cui contenuto minimo assicurerà l'imposizione di obblighi coerenti e compatibili con quelli previsti dall'Accordo sul trattamento dei dati personali stipulato con il Cliente e l'adozione di un medesimo livello di misure tecniche e organizzative. Il Produttore del Software rimarrà pienamente responsabile nei confronti del Cliente in relazione all'adempimento da parte del Sub-Responsabile degli obblighi dallo stesso assunti ai sensi dell'art. 28, par. 4, del Regolamento.

7.6. Al fine di fornire i Servizi, il Produttore del Software può avvalersi di Sub-Responsabili (quali, ad esempio, service providers multinazionali di servizi di hosting/data center), che forniscono i loro servizi sulla base di condizioni e termini contrattuali dagli stessi fissati e non negoziabili, anche per quanto concerne il trattamento dei dati (di seguito indicati come le "**Condizioni di Servizio del Sub-Responsabile**"). In tali circostanze, il Produttore del Software: i) da indicazione al Cliente del Sub-Responsabile di cui si avvale e delle relative Condizioni di Servizio del Sub-Responsabile; ii) presta ogni ragionevole sforzo al fine di assistere il Cliente nella verifica delle Condizioni di Servizio del Sub-Responsabile. Il Cliente può opporsi alla decisione della SWH di avvalersi del Sub-Responsabile, laddove sussistano ragioni tecniche connesse alla sicurezza e alle garanzie offerte dal Sub-Responsabile, secondo quanto previsto all'art. 7.3.

7.7. Ove il Produttore del Software svolga la sua attività in favore di un elevato numero di Clienti, le comunicazioni di cui all'art. 7.2 possono essere effettuate anche tramite la pubblicazione nell'area riservata agli Utenti indicati dal Cliente o altro mezzo ritenuto idoneo dal Responsabile che assicuri le esigenze di tutela del segreto industriale del Produttore del Software.

Articolo 8 – Trattamenti per i quali la SWH agisce in qualità di Titolare del trattamento

8.1. Il Produttore del Software agisce in qualità di Titolare del trattamento dei dati personali riferiti al Cliente, ove si tratti di persona fisica, e/o alle persone fisiche che sono i rappresentanti, esponenti, referenti, dipendenti e collaboratori del Cliente (ove si tratti di persona giuridica, ente o associazione), acquisiti per lo svolgimento delle proprie attività amministrative, contabili, organizzative e tecniche correlate o strumentali alla gestione del rapporto contrattuale con il medesimo Cliente (ad es., per la definizione e sottoscrizione del contratto, fatturazione dei servizi, gestione di accessi ed uso del Software Gestionale, gestione e manutenzione dei relativi sistemi e piattaforme, assistenza ed attività di help-desk a supporto degli Utenti del Cliente, ecc.). Per le attività di trattamento dei dati personali svolte in qualità di Titolare del trattamento, il Produttore del Software è tenuto al rispetto dei conseguenti obblighi previsti dal Regolamento[1], ad integrazione degli obblighi allo stesso direttamente spettanti quale Responsabile o Sub-Responsabile del trattamento in base al Regolamento e al Codice di condotta.

8.2. Il Produttore del Software, quale Titolare del trattamento, può trattare i dati personali riferiti al Cliente e ai relativi Utenti di cui al precedente art. 8.1 (raccolti attraverso l'accesso e l'uso del Software Gestionale e delle relative funzionalità) esclusivamente in forma aggregata, mediante il calcolo di opportune metriche e indicatori, per il perseguimento di legittimi interessi correlati a finalità statistiche, di analisi, studio e ricerca volte a migliorare la sicurezza, le prestazioni e le funzionalità dei medesimi Software e dei connessi Servizi, a beneficio anche degli stessi Clienti che ne fruiscono. Per tali finalità, l'elaborazione dei predetti dati personali è effettuata dal Produttore del Software previa adozione di tecniche di pseudonimizzazione o cifratura dei dati in modo tale da limitare la diretta riconducibilità delle informazioni agli Interessati, nonché sulla base della preventiva informativa fornita agli interessati circa le suddette finalità del trattamento e i legittimi interessi perseguiti.

8.3. Per le finalità sopra indicate l'informativa agli interessati può essere fornita dal Produttore del Software al Cliente e ai relativi Utenti in fase di sottoscrizione del contratto, anche in forma elettronica, attraverso la comunicazione di informazioni essenziali e sintetiche previamente all'accesso od utilizzo del Software e delle relative funzionalità, che possono rinviare ad un'informativa più estesa consultabile sul sito internet del Produttore secondo gli schemi esemplificativi di informative sintetica ed estesa predisposti dalla medesima Associazione e pubblicati nel sito internet dedicato al Codice di condotta, gestito dal Comitato Indipendente di Vigilanza di cui al successivo art. 19.2.

---

[1] *Ulteriori indicazioni e linee di indirizzo al riguardo potranno essere fornite nell'ambito del c.d. vademecum informativo reso disponibile da AssoSW agli operatori del settore in parallelo al CoC*

Articolo 9 - Registri dei trattamenti della SWH quale Responsabile del trattamento

9.1. Il Produttore del Software che agisce quale Responsabile del trattamento è tenuto a mantenere un registro delle attività di trattamento ai sensi dell'art. 30, par. 2, del Regolamento, a prescindere dal numero dei dipendenti dell'azienda o della natura dei dati trattati, in ragione del carattere non occasionale dei trattamenti svolti.

9.2. Considerato, tuttavia, che i Produttori del Software possono prestare la propria attività di Responsabili del trattamento in favore di un elevato numero di Clienti quali Titolari, nella tenuta e conservazione dei Registro delle attività di trattamento possono essere adottate le seguenti modalità:

a) indicazione dei Clienti Titolari del trattamento per conto dei quali sono effettuati i trattamenti, tramite il rinvio o il collegamento a schede o banche dati anagrafiche dei medesimi Clienti, con i relativi prodotti e/o servizi acquistati;

b) per quanto concerne gli altri elementi richiesti dall'art. 30, par. 2, la descrizione delle categorie dei trattamenti svolti può essere effettuata mediante rinvio a schede di servizio o a documentazione tecnica del prodotto o servizio.

9.3. Nelle ipotesi in cui il Produttore del Software agisce quale Sub-Responsabile del trattamento in favore di un Cliente che a sua volta opera quale Responsabile per conto di un terzo quale Titolare, nel Registro dei trattamenti della SWH, con specifico riferimento all'indicazione di cui al punto a) del precedente art. 9.2, può essere riportato solo il nominativo del Cliente quale Responsabile con cui intercorre il contratto di servizi e l'Accordo sul trattamento dei dati personali di cui all'art. 28 del Regolamento, considerato che in tali circostanze il Produttore del Software non intrattiene alcuna relazione contrattuale con il terzo Titolare e che l'identificazione dello stesso risulterebbe eccessivamente difficoltosa per il Produttore del Software.

9.4. Resta fermo, nelle ipotesi di cui al precedente art. 8, l'adempimento da parte del Produttore del Software dell'obbligo di tenuta ed aggiornamento di un registro delle attività di trattamento svolte quale Titolare ai sensi dell'art. 30, par. 1, del Regolamento.

Articolo 10 - Analisi dei rischi e valutazione d'impatto sulla protezione dati

10.1. Il Produttore del Software, per quanto di relativa competenza, avuto conto della natura dei dati, del tipo di trattamento effettuato nonché delle informazioni in suo possesso, coopera con il Cliente per permettergli di adempiere ai propri obblighi di legge in tema di analisi dei rischi e

valutazione d'impatto sulla protezione dati, fornendogli le informazioni concernenti le caratteristiche ed il funzionamento del Software Gestionale a livello tecnico, nonché le correlate funzionalità e misure di sicurezza. A tal fine, oltre alle informazioni già contenute nel contratto di servizio e nell'Accordo sul trattamento dei dati personali, il Produttore del Software potrà procedere alla fornitura di certificazioni, attestazioni e documentazioni tecniche e di sicurezza basate su standard di riferimento del settore, nonché dell'eventuale, ulteriore documentazione tecnica e di sicurezza predisposta dal medesimo Produttore a tal fine.

10.2. L'adozione, da parte del Produttore del Software, delle misure di cui agli Allegati A e B, è altresì volta a facilitare i Clienti nelle valutazioni condotte ex art. 24, 25, 32 e 35 del Regolamento. Il riferimento contenuto negli Allegati A e B alle disposizioni applicabili del Regolamento e alle norme internazionali tecniche di rilievo, permette al Cliente di condurre autonomamente le verifiche di conformità del Software Gestionale rispetto alle medesime misure.

10.3. Resta fermo, nelle ipotesi di cui al precedente art. 8, l'adempimento da parte del Produttore del Software, quale Titolare del trattamento, degli obblighi in tema di analisi dei rischi e adozione delle adeguate misure tecniche ed organizzative, nonché di valutazione d'impatto sulla protezione dati previsti dagli artt. 24, 25, 35 e 36 del Regolamento.

Articolo 11 - Misure adottate per la sicurezza del trattamento dei dati personali

11.1. Il Produttore di Software, ferma l'osservanza delle misure previste dall'Allegato A, si impegna a mettere in atto le misure previste dall'Allegato B nello svolgimento dei Servizi. Qualora il Software Gestionale sia utilizzato in modalità on premise, resta esclusa dalla responsabilità del Produttore del Software l'adozione delle misure idonee a proteggere le infrastrutture, i sistemi e i dispositivi utilizzati dal Cliente per accedere al Software (tra cui, ad esempio, le attività di salvataggio e backup dei dati personali e protezione dell'infrastruttura da malware).

11.2. Gli eventuali aggiornamenti e modifiche del Software Gestionale apportati via via nel tempo dal Produttore del Software, anche in rapporto all'evoluzione tecnologica non potranno comportare una riduzione del livello di sicurezza complessivo dei Servizi erogati e delle attività prestate.

11.3. Il Produttore del Software si impegna a mettere a disposizione in modo trasparente una descrizione delle misure di sicurezza applicate allo scopo di consentire al Cliente di valutare la rispondenza del Software Gestionale acquistato rispetto alle proprie esigenze e requisiti di sicurezza.

11.4. Nel caso in cui il Produttore del Software svolga attività tecniche riconducibili alle funzioni di amministratore di sistema, fermo quanto previsto al precedente art. 4.4, lo stesso Produttore provvede, nei termini individuati nell'Accordo sul trattamento dei dati personali con il Cliente,

all'attuazione di misure organizzative e tecniche adeguate nel rispetto del Provvedimento del Garante recante misure e accorgimenti in materia di amministratori di sistema.

11.5. Resta fermo, nelle ipotesi di cui al precedente art. 8, l'adempimento da parte del Produttore del Software, quale Titolare del trattamento, degli obblighi previsti dall'art. 32 del Regolamento.

Articolo 12 - Gestione degli incidenti di sicurezza

12.1. Il Produttore del Software assicura l'adozione di una procedura documentata che regolamenti la gestione degli incidenti di sicurezza che possano configurare una violazione dei dati personali (c.d. "**Data Breach**") ai sensi dell'art. 4, par. 1, numero 12) del Regolamento. La procedura deve definire nello specifico le azioni che il Produttore del Software, quale Responsabile del trattamento, deve porre in essere, nonché le informazioni che deve necessariamente fornire ai Clienti per consentire l'adempimento dei relativi obblighi ai sensi degli articoli 33 e 34 del Regolamento.

12.2 La procedura deve garantire l'adeguato e tempestivo coinvolgimento del Responsabile della Protezione dei Dati e delle funzioni interne (es. assistenza, IT, ricerca e sviluppo) interessate dall'incidente, nonché la tempestiva adozione di misure atte a limitare o mitigare l'impatto del medesimo sui trattamenti.

12.3. Qualora, in base alle verifiche interne condotte, risulti confermata con ragionevole grado di certezza l'esistenza della violazione, il Produttore del Software ne darà comunicazione al Cliente senza ingiustificato ritardo, e comunque, ove possibile, entro 48 ore, fermo restando che è esclusivo onere del Cliente, ove Titolare del trattamento, stabilire se l'incidente è classificabile come Data Breach e se il rischio per gli interessati è tale da richiedere la notifica all'Autorità di controllo e la comunicazione agli interessati coinvolti ai sensi dei richiamati articoli 33 e 34 del Regolamento. Sarà altresì onere del Cliente, qualora operi quale Responsabile del trattamento per conto di un Titolare del trattamento, informarlo tempestivamente non appena ricevuta la comunicazione della potenziale violazione da parte della SWH quale Sub-Responsabile di tale trattamento.

12.4. I Produttori del Software devono assicurare il rispetto degli obblighi del presente articolo anche da parte dei Sub-Responsabili di cui si avvalgono ai fini dell'erogazione dei Servizi al Cliente,

vincolandoli a comunicare alla Software House in modo tempestivo e senza ingiustificato ritardo eventuali incidenti di sicurezza, non appena ne siano venuti a conoscenza, con le modalità e entro il termine di cui al precedente art. 12.3.

12.5. Resta fermo, nelle ipotesi di cui al precedente art. 8, l'adempimento da parte del Produttore del Software, quale Titolare del trattamento, degli obblighi previsti dagli artt. 33 e 34 del Regolamento.

Art. 13 - Persone autorizzate operanti sotto il controllo della Software House

13.1 Il Produttore di Software assicura che il personale autorizzato al trattamento dei dati personali sia tenuto al rispetto di obblighi di riservatezza, anche relativi al periodo successivo alla conclusione del rapporto di lavoro, abbia accesso ai soli dati necessari per l'espletamento delle proprie attività lavorative e abbia ricevuto idonee istruzioni riguardo alle attività di trattamento allo stesso affidate, alle procedure adottate nonché in relazione ai diritti riconosciuti dal Regolamento. Il Produttore manterrà adeguata documentazione in ordine all'individuazione delle persone autorizzate al trattamento ed alle istruzioni alle stesse impartite, nonché in merito alla formazione impartita ai sensi dell'art. 13.2.

13.2. Il Produttore del Software eroga formazione del personale autorizzato in materia di protezione e sicurezza dei dati personali, erogata in diverse modalità presenza, *e-learning* e *fad* e periodicamente ripetuta in considerazione di fattori quali l'evoluzione tecnologica, normativa o a cambiamenti organizzativi.

Art. 14 - Assistenza al Cliente nella gestione delle richieste per l'esercizio dei diritti degli interessati

14.1 In relazione alle misure organizzative e tecniche da adottarsi al fine di prestare assistenza al Cliente, quale Titolare del trattamento, nel riscontro delle richieste di esercizio dei diritti degli interessati di cui al capo III del Regolamento, il Produttore di Software si impegna, ove tecnicamente possibile in base alle caratteristiche del Software Gestionale, a mettere a disposizione del Cliente funzionalità che gli consentono di effettuare le operazioni volte a rettificare, cancellare, accedere, estrapolare o esportare (ove necessario, in un formato strutturato, comunemente usato e leggibile da una macchina) i dati personali trattati per il tramite del medesimo Software, nonché a limitarne il trattamento, fornendo idonee informazioni esplicative al riguardo anche nell'ambito della documentazione tecnica resa disponibile al Cliente medesimo in ambito contrattuale. Laddove non sia possibile fornire, anche tenuto conto dello stato dell'arte e dei costi di attuazione, funzionalità di prodotto che consentano al Cliente di compiere le operazioni di trattamento cui sopra, il Produttore di Software si impegna a fornire al Cliente l'assistenza ragionevolmente necessaria per l'evasione delle richieste di esercizio dei diritti degli Interessati.

14.2. Laddove riceva direttamente richieste da parte di un interessato concernenti il trattamento di dati personali effettuato per conto del Cliente tramite i Servizi relativi al Software Gestionale, il Produttore di Software, quale Responsabile di tale trattamento, può invitare l'interessato a rivolgersi al Cliente quale Titolare o comunicare tempestivamente a quest'ultimo la istanza ricevuta dall'interessato, entro un termine ragionevole non superiore a 10 giorni lavorativi dalla loro ricezione. In relazione alle suddette richieste, anche ove ricevute direttamente dal Cliente, il Produttore si impegna comunque a collaborare con il Cliente, per quanto di relativa competenza, nella fornitura delle informazioni in suo possesso che possano risultare utili alla gestione della richiesta dell'interessato.

14.3. Resta fermo, nelle ipotesi di cui al precedente art. 8, l'adempimento da parte del Produttore del Software, quale Titolare del trattamento, degli obblighi previsti dagli artt. 15 – 22 del Regolamento.

Art. 15 - Trasferimento dei dati in Paesi terzi al di fuori della UE

15.1. Ai fini dello svolgimento dei Servizi oggetto del presente Codice, il Produttore del Software si impegna di regola a svolgere il trattamento dei dati personali mediante infrastrutture e piattaforme situate in Paesi della UE/SEE. Ove, per lo svolgimento di tali Servizi, si renda necessario per la SWH avvalersi, per ragioni organizzative e/o tecniche, anche di infrastrutture collocate in Paesi terzi al di fuori della UE/SEE o comunque di Sub-Responsabili, le cui attività possano comportare un trasferimento di dati personali al di fuori della UE/SEE, quest'ultima si impegna a:

a) svolgere il trattamento dei dati personali mediante infrastrutture e piattaforme situate in Paesi terzi per i quali:

   (i) la Commissione europea abbia comunque riconosciuto l'adeguatezza del livello di protezione dei dati personali garantito da tali Paesi, ai sensi dell'art. 45 del Regolamento;

   (ii) siano applicabili le garanzie appropriate o le ulteriori condizioni previste dai successivi artt. 46 e ss. del Regolamento;

b) avvalersi di Sub-Responsabili che svolgono il trattamento di dati personali nell'ambito del territorio dei suddetti Paesi, senza effettuare attività, servizi od operazioni, anche a livello tecnico, che comportino un trasferimento dei dati personali, trattati per conto del Cliente, al di fuori della UE/SEE, se non in accordo con il Cliente ed in presenza di misure di salvaguardia adeguate o garanzie supplementari, ove richieste.

15.2. Il Produttore del Software informa preventivamente il Cliente riguardo ad eventuali attività e servizi che possano comportare un trasferimento di dati personali in Paesi terzi al di fuori della

UE/SEE, fornendo indicazioni specifiche sul Paese di destinazione e sulla sussistenza di adeguate garanzie ai sensi degli artt. 44 – 49 del Regolamento, al fine di permettere al Cliente quale Titolare del trattamento di impartire le necessarie istruzioni mantenendo la documentazione atta a dimostrare le misure adottate in proposito.

15.3. Resta fermo, nelle ipotesi di cui al precedente art. 8, l'adempimento da parte del Produttore del Software, quale Titolare del trattamento, degli obblighi previsti dagli artt. 44 - 49 del Regolamento.

Art. 16 - Tempi di conservazione dei dati: cancellazione o restituzione dei dati al Cliente

16.1. Il Produttore del Software conserva i dati personali trattati per conto del Cliente in qualità di Responsabile del trattamento per tutta la durata dei Servizi e comunque per un tempo non superiore a quello necessario per la loro erogazione o a quello contrattualmente pattuito, sulla base delle istruzioni impartite dal Cliente e dell'Accordo sul trattamento dei dati personali con questo sottoscritto.

16.2. Alla cessazione del Servizio, per qualunque causa intervenuta, o in applicazione degli accordi intercorsi con il Cliente, il Produttore del Software è tenuto alla cancellazione dei dati personali dai propri sistemi o da quelli su cui lo stesso abbia controllo entro il termine previsto nel Contratto. Prima di procedere alla cancellazione, il Produttore del Software mantiene a disposizione del Cliente i dati personali per un periodo non inferiore a 30 (trenta) giorni successivi alla cessazione del Contratto, affinché lo stesso possa estrarne o chiederne copia secondo le modalità convenute con il Produttore del Software.

16.3. Il Produttore del Software ha la facoltà di conservare, anche in deroga ai termini indicati dal presente articolo, i dati personali che risultino necessari al fine di assolvere ad obblighi posti a proprio carico da una disposizione normativa italiana o europea in relazione ai Servizi svolti, ovvero quando la conservazione di tali dati sia consentita sulla base di una necessità esplicita, legittima e trasparente del medesimo Produttore (es. finalità di difesa e tutela giudiziaria del Responsabile o di attuazione e dimostrazione di misure di sicurezza implementate in relazione ai Servizi erogati).

Art. 17 - Richieste di informazioni e controlli del Cliente

17.1. Il Cliente deve essere in grado di valutare se le attività di trattamento del Produttore di Software sono conformi agli obblighi previsti dal presente Codice di condotta e dal Regolamento. A tal fine, il Produttore del Software si impegna a riscontrare tempestivamente, nei termini e secondo

le modalità di cui all'Accordo sul trattamento dei dati personali di cui al precedente art. 6, le richieste del Cliente volte ad ottenere le informazioni necessarie a dimostrare il rispetto degli obblighi assunti dal medesimo Produttore quale Responsabile del trattamento e a mettere a disposizione del Cliente tutte le informazioni necessarie per dimostrare la conformità alle disposizioni del Regolamento. Il Produttore di Software si impegna altresì a consentire lo svolgimento di verifiche da parte del Cliente sul trattamento dei dati effettuato dal medesimo Produttore ai fini dell'erogazione dei Servizi, in osservanza di quanto previsto a. 28, paragrafo 3, lett. h), del Regolamento.

17.2. Il Produttore del Software può decidere di affidare a auditor indipendenti la verifica di adeguatezza delle misure di sicurezza e protezione dei dati adottate con riguardo ai Servizi erogati. In questo caso, il diritto di verifica del Cliente può essere soddisfatto anche attraverso la messa a disposizione di tali report di verifica indipendente, che costituiscono informazioni riservate del Produttore del software, a condizione che tali verifiche:

a) siano eseguite in conformità ad uno standard di sicurezza riconosciuto (incluso, per esempio, le norme ISO/IEC 27001 27701, 27017, 27018, linee guida OWASP), da professionisti della sicurezza indipendenti e qualificati per eseguire tali audit (sulla base di una certificazione o esperienza riconosciuta);

b) siano documentate internamente attraverso un rapporto di audit, di cui al Cliente verrà fornito un documento di sintesi, che tenga conto delle esigenze di riservatezza, sicurezza e segreto industriale del Produttore del Software, al fine di permettergli di verificare il rispetto da parte del Produttore del Software degli obblighi di sicurezza e protezione dei dati, nell'ambito del Servizio, sullo stesso gravanti. Il rapporto di audit, sarà mantenuto internamente agli atti del Produttore per un periodo non inferiore ai dodici (12) mesi precedenti la richiesta di verifica e sarà reso disponibile all'Organismo di monitoraggio.

Art. 18 - Cooperazione con le Autorità di controllo, con l'Autorità giudiziaria e di polizia giudiziaria e tributaria

18.1. Il Produttore del Software, in qualità di Responsabile o Sub-Responsabile del trattamento, informa il Cliente in ordine alla ricezione di richieste di informazioni e documenti o comunque di accertamenti e controlli da parte del Garante, qualora abbiano ad oggetto il trattamento dei dati personali connesso all'erogazione dei Servizi al medesimo Cliente e, se del caso, può prestare ragionevole assistenza nel fornire le informazioni di cui è a conoscenza per i Servizi ed attività di relativa competenza.

a) 18.2. In caso di indagini, richieste di informazioni o verifiche ispettive avviate o svolte dalla Autorità giudiziaria o di polizia giudiziaria e tributaria, che comportino la comunicazione di dati personali trattati per conto del medesimo Cliente, il Produttore del Software si astiene dal darne informazione al Cliente, ove obbligato in base alla legge o al provvedimento dell'Autorità giudiziaria a garantire il segreto degli atti relativi alle suddette indagini.

Art. 19 - Verifiche sul rispetto del Codice di condotta ed organismo di monitoraggio

19.1. Fatti salvi i compiti e i poteri del Garante di cui agli articoli da 56 a 58 del Regolamento, per quanto attiene esclusivamente alle operazioni di trattamento di dati personali, il rispetto del presente Codice di condotta da parte dei Produttori del Software è garantito da un apposito Organismo di Monitoraggio (di seguito "**OdM**"), accreditato dal Garante per la protezione dei dati personali ai sensi dell'articolo 41 del Regolamento ed operante secondo quanto previsto dall'Allegato D del presente Codice di condotta.

Art. 20 - Modalità di adesione al Codice di condotta

20.1. I Produttori del Software, anche se non associati ad Assosoftware, possono presentare domanda di adesione al presente Codice di condotta per uno o più Software Gestionale dagli stessi prodotti, laddove ritengano che tali SW soddisfino i requisiti del medesimo Codice. A tal fine, inviano la domanda all'OdM, con le modalità, modulistiche e documentazione indicate nell'Allegato E del presente Codice di condotta. L'OdM procede alla verifica: (i) della regolarità e completezza della domanda e della documentazione presentate dal Produttore e (ii) della sussistenza dei requisiti di conformità del SW gestionale per cui si intende aderire (sulla base del questionario di autovalutazione compilato dal Produttore) e della dichiarazione relativa al rispetto degli impegni previsti dal Codice di condotta, nonché (iii) dell'assenza di condizioni ostative all'adesione da parte del Produttore richiedente. Ove necessario, l'Organismo può richiedere al Produttore di fornire gli ulteriori documenti ed informazioni necessari per regolarizzare e/o completare la domanda.

20.2. Entro trenta (30) giorni dalla ricezione della richiesta di adesione, ove le suddette attività di verifica abbiano esito positivo, l'OdM procede ad inviare al Produttore richiedente la comunicazione della conferma della adesione al Codice di condotta in riferimento al o ai SW per cui è stata richiesta e, contestualmente, a comunicare la nuova adesione al Garante, affinché possa aggiornare il registro di cui all'art. 40, paragrafo 6, del Regolamento. Per il primo anno decorrente dalla data di pubblicazione del provvedimento del Garante di approvazione del Codice di

condotta e di accreditamento dell'OdM, tale termine è fissato a centoventi (120) giorni dalla data di ricezione della domanda di adesione, in considerazione delle esigenze correlate alla prima fase di organizzazione e avvio delle attività dell'Organismo, chiamato a dotarsi di risorse adeguate al fine di esaminare un rilevante numero di domande di adesione.

20.3. L'eventuale mancata accettazione della domanda di adesione al Codice di condotta presentata da parte di un Produttore di software dovrà essere motivata da parte dell'OdM, fermo restando che tale diniego non preclude il successivo rinnovo della domanda di adesione che potrà essere presentata non prima di un anno dopo, unitamente ad una breve nota che illustri le misure adottate per superare le ragioni che avevano condotto al precedente diniego.

20.4 L'elenco dei Produttori Aderenti al Codice di condotta viene reso pubblico sul sito Internet a ciò dedicato, gestito dall'OdM.

Art. 21 – Riesame del Codice di condotta

a) 21.1 L'Associazione dei Produttori del Software (ASSOSOFTWARE), anche sulla base delle indicazioni e suggerimenti forniti dall'OdM, può in ogni momento promuovere il riesame del presente Codice di condotta e dei relativi Allegati, anche alla luce di novità normative, delle prassi applicative del Regolamento, del progresso tecnologico o dell'esperienza acquisita nella sua applicazione, sottoponendo le proposte di modifica all'approvazione del Garante ai sensi dell'art. 40 del Regolamento.

Art. 22 – Entrata in vigore del Codice di condotta

22.1 Il presente Codice di condotta, inserito nei registri di cui all'art. 40, paragrafi 6 e 11, del Regolamento, è pubblicato nella Gazzetta Ufficiale della Repubblica Italiana ed acquista efficacia il giorno successivo a quello della pubblicazione.

Allegato A

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
Requisiti sistemistici e di gestione	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

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

ALLEGATO B

Misure di sicurezza applicate dalle SWH per lo svolgimento dei Servizi riguardanti i SW Gestionali impiegati nei contesti on premise e in cloud

Nel presente Allegato B sono individuate le misure di sicurezza da adottare per lo svolgimento dei Servizi nei contesti on premise e in cloud, tenuto conto dei diversi e specifichi rischi da fronteggiare in tali distinti contesti.

Per le misure di sicurezza sono stati confrontati, sempre se applicabili alle attività di cui sopra:

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 necessari 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 confrontate con i parametri RID (riservatezza, integrità e disponibilità) utili per una valutazione degli impatti sugli interessati. Nella seconda sezione, le misure sono confrontate anche con il parametro Res (resilienza).

Misure di sicurezza applicate per lo svolgimento dei Servizi riguardanti i Software Gestionali impiegati nei contesti "on-premise"

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti	RID
Gestione Account	Autorizzazione e autenticazione	Tutti gli operatori della SWH devono accedere alle piattaforme utilizzate per l'assistenza previa autenticazione con le credenziali nominative individuali. Nel caso di un tentativo d'accesso alla piattaforma di supporto con un account diverso da quello autorizzato, il sistema deve negare l'accesso. Le utenze degli operatori incaricati dell'assistenza sono periodicamente revisionate allo scopo di verificare che i permessi e le autorizzazioni di accesso siano sempre aggiornate.	ISO/IEC 27002:2022 5.3, 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	RID
	Assegnazione dei privilegi	L'assegnazione dei privilegi agli operatori deve avvenire in base al principio del "need-to-know" e della "segregation of duties".		
	Password policy	Le password di accesso degli operatori incaricati dell'assistenza devono essere composte da almeno dodici (12) caratteri, prevedere caratteri alfanumerici e caratteri speciali, essere sostituite almeno ogni novanta (90) giorni, qualora si tratti di utenze privilegiate nella configurazione del SW, e conservate in formato crittografato.		
	Utilizzo della VPN	L'erogazione del servizio di assistenza e di accesso alla piattaforma da remoto devono avvenire mediante connessione VPN con MFA. La VPN può essere del Cliente o configurata dalla SWH in accordo col Cliente; prima dell'utilizzo di ogni sessione ci deve essere l'autorizzazione del Cliente che deve attivare o disattivare l'accesso ai propri sistemi in relazione alle attività svolte e richieste dallo stesso. Al termine dell'intervento l'operatore di assistenza dovrà	ISO/IEC 27002:2022 8.21	RID

		comunicare al Cliente la fine dell'intervento e richiedere la disattivazione dell'accesso.		
Gestione Sicurezza Logica	Patch Management	Continuo patching applicativo di sicurezza relativo alla piattaforma per l'erogazione del supporto da remoto.	ISO/IEC 27002:2022 8.8	RID
Log Management	Monitoraggio e gestione dei log di attività	Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate.	ISO/IEC 27002:2022 8.15 MM AgID ABSC 5.4.1, 5.1.1	R
Supporto da remoto in modalità attended (con presidio di un soggetto autorizzato da parte del Cliente)	Gestione dell'escalation interna	Gli operatori incaricati dell'assistenza devono accertarsi che le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Cliente (ad esempio tramite autenticazione sulla piattaforma di ticketing).	ISO/IEC 27002:2022 5.16 ISO/IEC 29100:2011 5.11	RID
	Gestione del sistema di supporto	Gli operatori incaricati dell'assistenza devono richiedere al Cliente in modo tracciabile le autorizzazioni necessarie ai fini dell'erogazione del servizio di assistenza (ad esempio, la condivisione dello schermo, il controllo condiviso dell'applicativo, il trasferimento dei file e la registrazione delle attività).	NA	R
Supporto da remoto in modalità unattended	Assegnazione dei privilegi da parte del Cliente	Deve essere garantita al Cliente la possibilità di assegnare specifici diritti ai determinati operatori incaricati dell'assistenza al fine di limitare l'accesso ai propri sistemi solo al personale autorizzato e per un intervallo temporale definito.	ISO/IEC 27002:2022 5.15,5.16 ISO/IEC 29100:2011 5.11	R

Supporto da remoto in modalità unattended	Accesso al DB	L'accesso agli ambienti di produzione da parte di Utenti che non operano in qualità di amministratori di sistema è consentito unicamente in presenza di comprovate esigenze di assistenza/manutenzione e mediante un processo autorizzativo ad hoc che consenta di tracciare la richiesta/autorizzazione del Cliente (es. “trouble ticketing”).	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
Attività di test	Utilizzo dei dati per l’esecuzione dei test	Utilizzo di dati fittizi (non dati reali) per l’esecuzione dei test. Solo in casi particolari, su richiesta del Cliente, ed in particolare quando sono sviluppate funzioni particolarmente complesse che devono essere provate e che devono essere verificate sull’esattezza della singola elaborazione e del singolo interessato presente negli archivi, prima di utilizzare gli archivi viene verificata l’adozione delle misure di sicurezza presenti negli ambienti di produzione. In questi casi i dati devono essere conservati per il tempo strettamente necessario all’esecuzione dell’attività di verifica della qualità e poi cancellati.	ISO/IEC 27002:2022 5.10	

	Accesso agli ambienti dei Clienti tramite IP pubblici	Il collegamento tramite IP pubblici su ambienti cloud dovrà avvenire da parte degli operatori incaricati dell'assistenza con utenze individuali, che dovranno essere attivate dal Cliente al fine di evadere la richiesta di assistenza. Solo nel caso in cui è previsto un servizio di assistenza continuativo tali credenziali potranno rimanere sempre attive, ma in questo caso gli accessi degli operatori dovranno essere loggati e l'operatore per ogni intervento dovrà giustificare la finalità per cui l'ha dovuto effettuare. Per tale finalità l'ambiente applicativo potrà prevedere utenze precaricate a sistema e le procedure di assegnazione delle stesse saranno in carico alla SWH in relazione alle esigenze segnalate dal Cliente.	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18 ISO/IEC 29100:2011 5.11	R
Gestione archivi	Autorizzazione per copia/trasferimento dati temporanei	L'eventuale copia o trasferimento di archivi o base dati del Cliente per finalità di assistenza o manutenzione deve essere preventivamente ed espressamente autorizzata dal Cliente stesso.	ISO/IEC 27002:2022 5.14	RI
	Secure disposal	I DB/archivi del Cliente devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di assistenza e immediatamente cancellati qualora non più necessari per l'esecuzione delle operazioni di assistenza.	ISO/ISO 27701: A.7.4.6	R

		Le copie dei DB/archivi del Cliente prelevati per finalità di assistenza devono essere trasferite tramite canali sicuri e protetti, salvate in ambienti dotati delle opportune misure di sicurezza e non devono essere sottoposti a backup allo scopo di minimizzare il trattamento.	ISO/IEC 27002:2022 5.14, 8.26 ISO/IEC 27701:2019 A.7.4.9	R
	Secure disposal	Qualora durante le attività di assistenza fosse necessario stampare documenti o informazioni, tali documenti devono rimanere nell'esclusiva disponibilità dell'operatore e da questi devono essere protetti contro accessi non autorizzati. Al termine dell'attività, i documenti dovranno essere distrutti.	ISO/ISO 27701: A.7.4.6	R

	Attività di migrazione e conversione	In relazione alle attività di migrazione dei dati sono da prevedere le seguenti misure di sicurezza: - Utilizzo di canali sicuri e protetti nella trasmissione dei dati; - Utilizzo delle basi dati contenenti dati effettivi in ambiente dedicato, dotato di misure di sicurezza idonee a garantirne la riservatezza; - Configurazione dei profili di accesso a tali ambienti al solo personale preposto dalla SWH alla gestione delle attività di migrazione compreso il test ed il collaudo. Ove richiesto, tali profili sono estesi anche al personale del Cliente. Qualora presenti, gli accessi da remoto avvengono sempre mediante l'utilizzo di canali sicuri; - Conservazione dei dati esclusivamente fino al buon fine del completamento delle attività di verifica ed alla conseguente consegna, approvazione e accettazione da parte del Cliente.	ISO/IEC 27002:2022 5.14, 5.15, 8.26 ISO/IEC 27701:2019 A.7.4.9	RI

Governance	Tracciabilità	Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing).	ISO/IEC 27002:2022 5.10	RID
Governance	Data Breach	Sono adottate procedure di gestione degli incidenti che consentono di individuare, contenere e risolvere situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5,27	RID

Misure di sicurezza applicate per lo svolgimento dei Servizi riguardanti i Software Gestionali impiegati nei contesti in cloud

Le misure che seguono devono essere applicate dalla SWH qualora il Software Gestionale sia utilizzato dal Cliente attraverso il Data Center della medesima SWH, oppure tramite Data Center esterni resi disponibili da sub-fornitori della SWH, di cui quest'ultima mantiene comunque la gestione amministrativa dei sistemi di erogazione della soluzione informatica. Qualora il servizio fosse erogato da Data center esterni che assumono anche la gestione sistemistica dei server e dell'infrastruttura necessari all'erogazione dei servizi, la SWH provvederà a vincolare il sub-fornitore al rispetto di misure di sicurezza a livello contrattuale e sottoporrà il DC esterno ad audit periodici per la verifica della relativa applicazione.

Ambito	**Catalogazione**	**Requisito di dettaglio**	**Riferimenti**	**RID Res**
Misure sicurezza Data Center	Accesso al Sistema o SW (autenticazione)	Adozione di misure dirette a garantire che: - gli accessi di amministrazione da parte della SWH siano riservati al personale a cui sia attribuita la qualifica ("ruolo") di amministratore di sistema, in virtù di elevate capacità tecniche e caratteristiche di comprovata affidabilità e moralità ; - l'accesso amministrativo ai sistemi da parte del personale del Cliente avverrà attraverso procedure di autenticazione a più fattori (MFA).	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18, 8.15 MM AgID ABSC 5.1.1, 5.4.1, 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RID

Misure sicurezza Data Center	Accesso al Sistema o SW (policy di gestione)	Per i servizi che prevedono una modalità di gestione amministrativa delle componenti infrastrutturali, devono essere previste le seguenti policy: - utenze che consentono l'individuazione dell'amministratore che esegue l'intervento; - attivazione di un processo di log management che identifichi i log in, log out e log in failed; - conservazione dei log in un formato che ne garantisca l'integrità e la lettura nel tempo; - conservazione dei log per almeno sei (6) mesi; - verifica annuale dell'operato degli amministratori di sistema; - accesso ai sistemi attraverso VPN e MFA.	ISO/IEC 27002:2022 5.3	
Misure sicurezza Data Center	Log Management	Funzionalità per il tracciamento o registrazione (log) degli accessi e delle attività svolte dagli Utenti. I log concernenti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore di sistema del Cliente o della Software House su richiesta del Cliente.	ISO/IEC 27002:2022 8.15	R

Misure sicurezza Data Center	Auditing	Utilizzo del sistema di gestione e analisi dei log anche per il monitoraggio delle attività degli amministratori di sistema. L'accesso al sistema di gestione dei log è riservato al personale avente ruolo di auditor e non è ammesso per il personale addetto all'amministrazione di sistema.	ISO/IEC 27002:2022 8.16	R
Misure sicurezza Data Center	Crittografia dei protocolli di comunicazione	Applicazione di protocolli crittografici standard di comunicazione sicuri e non obsoleti, nei casi in cui l'accesso al sistema sia effettuato tramite Internet.	ISO/IEC 27002:2022 5.14, 8.21 ISO/IEC 29100:2011 5.11	RI
Misure sicurezza Data Center	Minacce e Vulnerabilità	Adozione di un programma di gestione delle minacce e dei rischi per monitorare continuamente le vulnerabilità delle Piattaforme SaaS indicate da best practice internazionali attraverso la pianificazione e l'esecuzione di scansioni delle vulnerabilità interne ed esterne e test di penetrazione. Le vulnerabilità identificate devono essere valutate per determinare i rischi associati e le opportune azioni correttive stabilite in base alla priorità assegnata e gravità rilevata.	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 Res
Misure sicurezza Data Center	Firewalling	Adozione di sistemi di firewall finalizzati a filtrare e contenere il traffico identificando eventuale traffico anomalo indicatore di possibili attacchi informatici. Presenza di firewall L4 o L7/WAF.	ISO/IEC 27002:2022 5.14, 8.22 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Intrusion Prevention	Protezione dell'ambiente mediante cui è erogato il servizio dalla SWH mediante Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito.	ISO/IEC 27002:2022 7.4, 8.21 ISO/IEC 29100:2011 5.11	RID Res

Misure sicurezza Data Center	Malware protection	Adozione di misure di protezione da infezioni di software malevolo, di difesa da azioni non autorizzate, da applicazioni sospette e di protezione da tentativi di sottrazione di dati personali (es. mediante sistemi antivirus, antispamming, antiphishing, etc., mantenuti costantemente aggiornati).	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Filesystem Antivirus	Adozione di moduli Antivirus sul filesystem su tutti i server utilizzati per la fornitura dei servizi, con possibilità di configurare, su base progettuale, prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11	RD
Misure sicurezza Data Center	Monitoraggio e gestione incidenti	Adozione di policy e procedure per l'identificazione, gli interventi, i rimedi e le segnalazioni di incidenti che determinano un rischio per l'integrità o riservatezza dei dati personali o altre violazioni della sicurezza.	ISO/IEC 27002:2022 5.24, 5.25, 5.26, 5.27, 5.28, 6.8	RID Res
Misure sicurezza Data Center	Security Patch Management	Sottoposizione della piattaforma ad un processo periodico di verifica delle patch o delle fix disponibili relativamente alle componenti dell'impianto di erogazione e a quelle ritenute critiche per l'erogazione del servizio o per la sicurezza.	ISO/IEC 27002:2022 8.8 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Sicurezza fisica	Applicazione di adeguate misure di sicurezza fisica alla piattaforma hardware/software progettata (es. utilizzo di hosting providers/servizi di data center dotati di adeguati sistemi di prevenzione del rischio intrusione, incendio, allagamento, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res

Misure sicurezza Data Center	Anti allagamento	Adozione nell'ambito del Data Center di tutte le misure necessarie a prevenire allagamenti (quali presenza di sonde, impianti di allarme, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res
Misure sicurezza Data Center	Anti intrusione	Impostazione nel Data Center di un sistema di controllo degli accessi che identifichi coloro che accedono e impedisca l'accesso ai non autorizzati. La procedura deve prevedere anche la gestione del Change con l'attivazione e disattivazione dell'autorizzazione all'accesso in funzione dei cambi di ruolo.	ISO/IEC 27002:2022 7.1, 7.2 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Telecamere a circuito chiuso	Installazione di telecamere (CCTV) per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.	ISO/IEC 27002:2022 7.4 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Condizionamento	Adozione di adeguati impianti di condizionamento e di raffreddamento degli ambienti ed apparati.	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res
Misure sicurezza Data Center	Continuità ed emergenza	Adozione di procedure e controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema/SW (in caso di incidente / violazione di dati personali). Le procedure devono comprendere le indicazioni per la conservazione delle copie di backup nonché un piano per il disaster recovery.	ISO/IEC 27002:2022 5.4, 5.29 MM AgID ABSC 10 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Cancellazione dei dati	Previsione di misure per la cancellazione dei dati di produzione al termine dell'erogazione del servizio secondo i termini contrattuali definiti con il Cliente.	ISO/IEC 27002:2022 8.10	R
Misure sicurezza Data center esterni	Verifica dei requisiti del sub-fornitore e contrattualizzazione degli obblighi relativi alle misure di sicurezza	Selezione e verifica dei requisiti del sub-fornitore che assume la gestione sistemistica dei server e dell'infrastruttura necessari allo svolgimento dei	ISO/IEC 27002:2022 5.19; 5.20	RID

		Servizi e sottoscrizione di un contratto che vincoli il medesimo sub-fornitore al rispetto degli obblighi concernenti le misure di sicurezza (previsti dalla SWH per la gestione del DC).		
Misure sicurezza Data center esterni	Audit nei confronti del sub-fornitore	Sottoposizione del sub-fornitore che gestisce il DC esterno ad audit periodici per la verifica del rispetto degli obblighi concernenti le misure di sicurezza, fatto salvo quanto previsto dalle condizioni di servizio fissate da providers multinazionali di servizi di DC ai sensi dell'art. 7.7 del CoC.	ISO/IEC 27002:2022 5.22	RID
Connettività	Linee Internet e disponibilità di banda	Previsione di misure volte ad assicurare una connettività adeguata in conformità ai livelli di servizio contrattualmente definiti con il Cliente.	ISO/IEC 27002:2022 8.6, 8.21	RI
Connettività	Firewalling	Protezione dell'accesso ai sistemi contro il rischio d'intrusione attraverso adeguate misure di firewalling.	ISO/IEC 27002:2022 5.14, 8.22, 8.21, 8.23 ISO/IEC 29100:2011 5.11	RID
Sicurezza rete	AntiDDoS	Erogazione da parte del Data Center di un servizio in grado di rispondere in modo efficace alle problematiche create dagli attacchi ("**DDoS**").	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11	D
Sicurezza rete	IDS/IPS	Adozione di un sistema IPS (Intrusion Prevention System) in grado di bloccare automaticamente gli attacchi rilevati e IDS (Intrusion Detection System) in grado di intercettare le minacce fornendo così una protezione real-time ai servizi erogati dal Data Center.	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11	RD
Governance	Formazione	Erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali ai propri dipendenti coinvolti nelle attività di trattamento.	ISO/IEC 27002:2022 6.3	na

Governance	Ubicazione geografica	Dichiarazione da parte della SWH nei confronti del Cliente dell'ubicazione geografica del DC e dei dati.	ISO/IEC 27002:2022 5.31	na
Governance	Data Breach	Adozione di procedure di individuazione, contenimento e risoluzione di situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5,27	RID
Requisiti sistemistici e di gestione	Sicurezza logica	Rivalutazione con cadenza almeno annuale delle misure e procedure di sicurezza applicate in modo da aggiornarle in relazione alle vulnerabilità rilevate, agli attacchi subiti e all'evoluzione della tecnologia.	ISO/IEC 27002:2022 8.27 MM AgID ABSC 3.1.2	RI

Allegato C

SCHEMA DI ACCORDO SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679 – REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI [1]

TRA

_____ (*indicare Cliente*) con sede legale in _____ (di seguito anche il "**Cliente**"),

da una parte,

E

_____ (*indicare SWH*) con sede legale in _____ (in seguito anche la "**Software House**" o "**SWH**"),

dall'altra parte,

(il Cliente e la SWH, indicati di seguito, singolarmente, come la "**Parte**" e, collettivamente, come le "**Parti**").

Premesso che:

1. le Parti hanno sottoscritto un contratto (di seguito "**Contratto**") di concessione della licenza d'uso del Software gestionale sviluppato e prodotto dalla SWH e di svolgimento dei Servizi di cui all'art. 2, comma 1, lett. c) del Codice di condotta, come specificati nel Contratto che possono comportare operazioni di trattamento di dati personali eseguite dalla medesima SWH per conto del Cliente;
2. in relazione alle suddette operazioni di trattamento di dati personali, il Cliente riveste dunque il ruolo di Titolare del trattamento [o di "Responsabile del trattamento"][2], mentre la SWH opera in qualità di Responsabile del medesimo trattamento [*o di* "Sub-responsabile del trattamento"][3] ai sensi dell'art. 28 del Regolamento (UE) 2016/679 - Regolamento Generale sulla Protezione dei Dati (di seguito il "**Regolamento**" o "**GDPR**");
3. in particolare, la SWH dichiara, ai sensi dell'art. 28, comma 5, del GDPR, di aderire al "Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale" (di seguito il "**Codice di condotta**") e pertanto dichiara di mettere in atto misure tecniche ed organizzative adeguate al fine di garantire che il suddetto

---

[1] *Si riporta qui di seguito il testo esemplificativo di articolo da inserire nel Contratto con il Cliente, contenente il rinvio allo schema di Accordo sul trattamento dei dati personali da allegare al medesimo Contratto:*
"***Art. … - Trattamento dei dati personali***
In relazione al trattamento dei dati personali connesso allo svolgimento dei Servizi, il Fornitore conferma di svolgere tale trattamento in qualità di Responsabile/Sub-responsabile per conto del Cliente, quale Titolare/Responsabile del medesimo trattamento, e, ai sensi dell'articolo 28 del Regolamento, si impegna a garantire il rispetto degli obblighi previsti nell'Accordo sul trattamento dei dati personali di cui all'Allegato …, contenente anche la descrizione del suddetto trattamento dei dati personali. (…)".

[2] *Sostituire con "Responsabile del trattamento", ove il Cliente agisca invece in tale qualità per conto di un soggetto terzo quale Titolare, adeguando anche le successive parti in cui si indica il Cliente quale Titolare del trattamento (da sostituire, in tal caso, con "Responsabile del trattamento").*

[3] *Inserire "ulteriore Responsabile del trattamento (di seguito "Sub-Responsabile")", ove, come indicato al precedente commento, il Cliente agisca già quale Responsabile del trattamento e uniformare anche tutte le successive parti (sostituendo il termine di "Responsabile" riferito alla SWH con "Sub-Responsabile")*

trattamento di dati personali sia effettuato nel rispetto di quanto previsto dal GDPR e dal Decreto Legislativo n. 196/2003 e s.m.i. – Codice in materia di protezione dei dati personali (di seguito, il "**Codice privacy**");

4. il Cliente prende atto che la presente proposta di accordo è formulata sulla base dello schema di Accordo sul trattamento dati ex art. 28 del GDPR, di cui all'Allegato C del suddetto Codice di condotta.

Tutto ciò premesso, con la sottoscrizione del presente accordo (di seguito "**Accordo**"), le Parti convengono quanto segue.

1. Premesse

1.1. Le premesse costituiscono parte integrante e sostanziale del presente Accordo.

2. Oggetto dell'Accordo

2.1. Con il presente Accordo le Parti convengono di disciplinare gli obblighi assunti dalla SWH quale Responsabile del trattamento[4] dei dati personali effettuato per conto del Cliente, quale Titolare, nello svolgimento dei Servizi oggetto del Contratto.

3. Descrizione del trattamento dei dati personali

3.1. La esecuzione dei Servizi oggetto del Contratto comporta, da parte della SWH, il trattamento di dati personali descritto nell'Allegato A del presente Accordo.

4. Obblighi della SWH

4.1. Fermi gli obblighi che le disposizioni del GDPR e le previsioni del Codice di condotta pongono direttamente a carico della SWH quale Responsabile del trattamento[5], quest'ultima si impegna ad osservare e a far osservare al proprio personale i seguenti obblighi:

a) trattare i dati personali soltanto sulla base delle documentate istruzioni fornite dal Cliente, ad integrazione di quanto già previsto dal Codice di condotta … [*anche in caso di eventuale trasferimento di dati personali verso soggetti stabiliti in Paesi al di fuori della UE, che potrà essere effettuato solo previa autorizzazione del Titolare medesimo e sulla base delle relative istruzioni, adottando le adeguate garanzie secondo la vigente normativa europea e nazionale di riferimento, garanzie di cui andrà mantenuta adeguata documentazione da fornire, ove richiesto, al Cliente*][6];
b) individuare le persone autorizzate al trattamento dei dati personali che operano sotto la propria autorità e fornire loro adeguate istruzioni per lo svolgimento delle attività di trattamento verificandone l'osservanza anche con riferimento agli obblighi di riservatezza, nel rispetto di quanto previsto dall'art. 13 del Codice di condotta;
c) adottare gli standard e misure per la sicurezza dei dati personali previsti dal Codice di condotta e, in particolare, dai relativi Allegati A e B, vigilando sulla applicazione delle stesse, in modo da ridurre al minimo i rischi di violazioni dei dati personali. Qualora il Cliente richieda

---

[4] V. note 1 e 2
[5] V. nota 2
[6] Facoltativo: si può eliminare per SWH che non abbiamo operatività con estero o rapporti con soggetti (subfornitori, partner, ecc.) stabiliti extra UE

di adottare misure di sicurezza aggiuntive, la SWH si riserva il diritto di valutarne la fattibilità e potrà applicare costi aggiuntivi a carico del Cliente per tale implementazione;

d) assistere il Cliente, per quanto di relativa competenza, nel garantire il rispetto degli obblighi in tema di sicurezza, di notifica al Garante per la protezione dei dati personali di eventuali violazioni dei dati personali e, se del caso, comunicazione agli interessati, nonché di valutazione d'impatto sulla protezione dati ed eventuale consultazione preventiva, ai sensi degli articoli da 32 a 36 del GDPR, tenendo conto di quanto già previsto in proposito dagli articoli 10, 11 e 12 del Codice di condotta, nonché della natura del trattamento e delle informazioni a disposizione della stessa SWH;
e) comunicare al Cliente per iscritto, senza indebito ritardo, eventuali incidenti di sicurezza che possano configurare una violazione dei dati personali trattati ai fini della esecuzione dei Servizi oggetto del Contratto, provvedendo alla relativa gestione secondo quanto previsto dall'art. 12 del Codice di condotta. Tutte le informazioni ricevute dal Cliente in occasione della comunicazione della violazione da parte del Produttore di Software dovranno essere considerate informazioni riservate e potranno essere comunicate a terzi solo per adempiere ad obblighi imposti dalla normativa vigente;
f) collaborare con il Cliente per l'evasione delle richieste degli interessati di esercizio dei diritti previsti dagli artt. 15-22 del GDPR, informando prontamente il Cliente in caso di ricezione di eventuali richieste da parte degli interessati, nel rispetto di quanto previsto dall'art. 14 del Codice di condotta[7];
g) informare tempestivamente il Cliente in caso di ricevimento di richieste di informazioni o documenti, accertamenti ed ispezioni, da parte del Garante per la protezione dei dati personali, quale autorità competente di controllo, o di altre autorità giudiziarie o di polizia giudiziaria, ove attinenti al trattamento dei dati personali connesso alla esecuzione delle Servizi oggetto del Contratto, fatto salvo, ai sensi dell'art. 18, comma 2, del Codice di condotta, il rispetto degli obblighi di segreto previsti dalla legge o dal provvedimento dell'Autorità giudiziaria, e collaborare con il Cliente, quale Titolare, alla predisposizione dei correlati riscontri, atti, documenti o comunicazioni, secondo quanto previsto dall'art. 18 del Codice di condotta;
h) cancellare tutti i dati personali trascorsi trenta (30) giorni dopo la cessazione dei Servizi oggetto del Contratto e cancellare le copie esistenti, o restituirli al Cliente su richiesta di quest'ultimo, secondo quanto previsto dall'art. 16 del Codice di condotta, salvo che la vigente normativa europea o nazionale preveda la conservazione dei dati da parte della SWH che, in tal caso, ne darà contestuale attestazione al Cliente;
i) nel caso di richieste di informazioni e di controlli da parte del Cliente, che comportino l'accesso a documenti o informazioni aziendali riservate, la SWH, posto quanto previsto dall'art. 17 del Codice di condotta, per assicurare la tutela dei relativi interessi industriali e commerciali, nonché la sicurezza dei relativi Prodotti e Servizi, potrà prevedere che lo svolgimento delle verifiche sia subordinato all'adozione di specifici impegni di riservatezza da parte del Cliente e dei soggetti da questi eventualmente incaricati (es. auditor, revisori, etc.). In ogni caso, le tempistiche e le modalità di svolgimento delle verifiche dovranno essere preventivamente concordate con la SWH, allo scopo di salvaguardarne sia le politiche di riservatezza e di accesso ai locali aziendali, sia le esigenze di continuità operativa e

[7] *Valutare se inserire nel Contratto la seguente previsione: "Laddove alla SWH sia richiesto uno sforzo superiore a quello ragionevolmente necessario per dare supporto nella gestione e riscontro di richieste degli interessati, la medesima SWH potrà addebitare al Cliente un costo ragionevole basato sulle spese amministrative da sostenere effettivamente per il supporto fornito"*

l'assenza di conflitti di interesse rispetto ai soggetti incaricati delle attività di verifica. La SWH potrà concordare con il Cliente eventuali costi ragionevolmente necessari all'espletamento di specifiche attività di verifica dallo stesso richieste in materia di protezione dati, che comportino comunque il coinvolgimento di personale del Produttore e che abbiano una durata superiore alla giornata lavorativa.

5. Ricorso della SWH a Sub-Responsabili del trattamento

5.1. La SWH, nel rispetto di quanto previsto all'art. 7 del Codice di condotta, è autorizzata in via generale[8] ad avvalersi di ulteriori Responsabili (di seguito "**Sub-Responsabili**") appartenenti alle seguenti categorie: …

5.2. L'elenco completo dei Sub-Responsabili è reso disponibile al Cliente a richiesta e/o tramite la relativa area riservata o i canali di assistenza. La SWH può sostituire gli ulteriori Responsabili in qualsiasi momento, previa comunicazione scritta al Cliente o aggiornamento del menzionato elenco. Il Cliente potrà manifestare la sua opposizione entro trenta (30) giorni dal ricevimento dalla comunicazione o dall'aggiornamento dell'elenco.

5.3. La SWH dichiara e garantisce che tali Sub-Responsabili presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni del GDPR e si impegna a vincolare contrattualmente gli ulteriori Responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dalla SWH nei confronti del Cliente.

5.4. Il Produttore del Software rimarrà pienamente responsabile nei confronti del Cliente in relazione all'adempimento da parte del Sub-Responsabile della SWH degli obblighi dallo stesso assunti ai sensi dell'art. 28, par. 4, del GDPR.

6. Durata dell'Accordo

6.1. Il presente Accordo ha la stessa durata del Contratto e verrà meno in tutti i casi di cessazione del Contratto medesimo.

7. Modifiche

7.1. Nessun accordo o pattuizione che modifichi o ampli il presente Accordo sarà vincolante per le Parti, salvo che sia effettuato per iscritto, si riferisca espressamente al presente Accordo, sia sottoscritto e scambiato tra le Parti.

8. Effetti del presente Accordo

8.1. Il presente Accordo supera ed annulla altre eventuali intese o accordi precedenti delle Parti, aventi lo stesso oggetto.

8.2. Per tutto quanto non disciplinato dal presente Accordo le Parti convengono di fare riferimento al Contratto.

9. Comunicazioni

9.1. Ad eccezione di quanto espressamente previsto all'articolo 4, qualsiasi comunicazione prevista o consentita ai sensi del presente Accordo dovrà avvenire per iscritto via posta elettronica certificata

[8] Verificare coerenza con eventuale clausola contrattuale concernente la deroga al divieto di subappalto delle attività

(PEC) agli indirizzi indicati nel Contratto, e si considera validamente effettuata al momento del ricevimento della comunicazione dalla Parte destinataria.[9]

… (*luogo*), … (*data*)

IL CLIENTE
… (*nominativo e qualifica*)
Firma .....

LA SOFTWARE HOUSE
… (*nominativo e qualifica*)
Firma .....

[9] *Valutare se, ove non già previsto, inserire nell'ambito del Contratto anche le seguenti previsioni:*
*"**... Remunerazione** - Le Parti hanno già tenuto in debito conto le attività che la SWH avrebbe svolto in qualità di Responsabile nella determinazione della remunerazione prevista nel Contratto. Le Parti convengono che, in virtù del presente Accordo, la SWH non riceverà alcuna remunerazione, indennità o compenso specifico ed ulteriore rispetto a quello previsto dal Contratto.*
*… **Garanzia e manleva -** Le Parti si impegnano comunque a tenersi reciprocamente indenni e manlevate per ogni danno, onere, costo, spesa e/o pretesa di terzi eventualmente derivante dalla violazione delle disposizioni del GDPR e del Codice Privacy, che risultino rispettivamente imputabili.*"

Allegato A

Descrizione delle attività di trattamento di dati personali connesse allo svolgimento delle Attività oggetto del Contratto

Attività svolte	**Finalità del trattamento**	**Natura del trattamento**	**Durata del trattamento**	**Categorie di interessati**	**Categorie di dati personali**
Es.: installazione, test, collaudo, messa in esercizio, assistenza, manutenzione, aggiornamento del SW Gestionale …	…	*Interamente/ parzialmente automatizzata*	*Es.: Durata del Contratto*	*Es.: clienti, utenti, dipendenti, ecc.*	*Es.: dati personali comuni, dati particolari, dati penali (specificare sotto categorie*) …

ALLEGATO D – ORGANISMO DI MONITORAGGIO

Organismo di Monitoraggio

1. L'OdM è un soggetto esterno all'organizzazione di Assosoftware che abbia ottenuto l'accreditamento da parte del Garante per la protezione dei dati personali (di seguito, il "**Garante**" o anche l'"**Autorità**") ai sensi dell'art. 41 del Regolamento (UE) 2016/679. L'OdM e è composto da un numero di tre componenti, designati, rispettivamente, uno dal Consiglio Generale di Assosoftware, quale soggetto promotore del Codice di condotta sulla base delle candidature proposte dai Produttori del Software associati, uno dagli organismi rappresentativi delle categorie dei Clienti utilizzatori dei SW Gestionali e uno dal CNCU insieme alle associazioni maggiormente rappresentative degli interessati a livello nazionale, sulla base di candidature relative a persone provenienti da ambienti accademici, tecnici o legali con comprovata esperienza in materia di protezione dei dati personali e sicurezza delle informazioni con riguardo anche al settore relativo al Software Gestionale, a condizione che si tratti di persone esterne all'Associazione, che non abbiano partecipato ai lavori di stesura del presente Codice di condotta e che rispettino i requisiti di onorabilità, indipendenza, imparzialità, conflitto di interessi e competenza sotto indicati per i componenti degli OdM. L'OdM sarà comunque presieduto dal componente designato da Assosoftware, quale persona di riconosciuta esperienza in materia di protezione e sicurezza dei dati personali, con particolare riguardo al settore dei Software Gestionali, che svolgerà funzioni di supervisione e cura del coordinamento e dell'organizzazione delle attività dell'Organismo medesimo.

L'incarico dei componenti dell'OdM, avrà la durata di cinque (5) anni, non rinnovabile. Prima della scadenza del mandato dell'OdM, Assosoftware provvederà a richiedere l'accreditamento dell'organismo nella nuova composizione. Per le relative attività amministrative e di segreteria, l'OdM può avvalersi del supporto di personale reclutato tramite agenzie esterne di lavoro e/o messo a disposizione da Assosoftware, purché esclusivamente dedicato alle attività dell'Organismo e operante sotto il diretto controllo di quest'ultimo (senza alcuna ingerenza da parte della stessa Associazione). Laddove l'OdM, ai fini di un efficiente svolgimento dei propri compiti, avesse necessità di personale di supporto, il relativo incarico potrà essere affidato anche a consulenti o collaboratori esterni in possesso di adeguate competenze nella materia oggetto del presente Codice di condotta e in relazione allo specifico settore delle Attività di Sviluppo dei Software Gestionali e/o dei Servizi concernenti l'impiego di tali SW, come definiti all'art. 2.2., lettere c) e d), del Codice medesimo.

2. I componenti dell'OdM devono garantire e mantenere per l'intera durata dell'incarico i seguenti requisiti:

a) **Onorabilità**: non possono (i) trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile; (ii) essere stati radiati da albi professionali per motivi disciplinari o per

altri motivi; (iii) aver riportato condanna, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per uno dei delitti previsti dal R.D. 16 marzo 1942, n. 267 (legge fallimentare), o per uno dei delitti previsti dal titolo XI del Libro V del codice civile, o per un delitto non colposo, per un tempo non inferiore ad un anno, per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica; (iv) aver riportato una condanna, anche non definitiva, per uno dei reati previsti dal D.lgs. n. 231/2001 e s.m.i.; (v) fermo quanto sopra disposto e salvi gli effetti della riabilitazione, essere stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria, ovvero condannati con sentenza irrevocabile per un qualsiasi reato.

b) **Indipendenza e imparzialità**: Al fine di garantire la piena indipendenza e imparzialità dei componenti dell'OdM, evitando qualsiasi forma di interferenza, condizionamento o conflitto di interessi, è previsto che, sia l'Organismo nel proprio complesso, che i singoli componenti, non debbano subire alcuna ingerenza nell'esercizio delle proprie attività da parte di Assosoftware e dei Produttori del Software aderenti al presente Codice di condotta. Nello svolgimento delle proprie funzioni di controllo, inoltre, l'OdM non sarà soggetto, in via diretta o indiretta, ad alcuna forma di controllo, direzione o vigilanza da parte di Assosoftware, dei Produttori aderenti o eventualmente riconducibili al settore dei Software Gestionali. L'OdM adotterà le proprie decisioni senza che alcuno degli organi di Assosoftware possa sindacarle.

c) **Conflitto d'interessi**: Ciascun componente dell'OdM deve costantemente garantire la massima imparzialità ed indipendenza anche evitando ogni situazione di conflitto di interessi, reale o anche solo potenziale, sia per sé stesso che in riferimento a propri parenti, affini entro il terzo grado, coniugi o conviventi. A tal fine, ogni componente dovrà inderogabilmente dichiarare senza alcun ingiustificato ritardo, in qualunque momento nel corso dell'esecuzione dei propri compiti di cui al presente Codice di condotta, qualsiasi circostanza in grado di configurare o comunque determinare un conflitto di interessi, conseguentemente astenendosi dal prendere parte a qualsiasi processo decisionale e dal compiere qualsivoglia attività in seno all'OdM per cui rilevi il conflitto di interessi che lo vede coinvolto.

d) **Competenza**: Ai fini di un corretto ed efficiente svolgimento dei propri compiti, è essenziale che ciascun componente dell'OdM garantisca un adeguato livello di competenza, da intendersi come l'insieme delle conoscenze, delle esperienze e degli strumenti necessari ad un efficiente svolgimento delle funzioni assegnate. Per tale ragione, i componenti dovranno avere, anche nel loro insieme come Organismo: (a) un'approfondita conoscenza ed esperienza (di tipo giuridico e informatico) in materia di protezione dei dati personali; (b) un'approfondita conoscenza ed esperienza nelle Attività di Sviluppo dei Software Gestionali e/o nello svolgimento dei Servizi concernenti l'impiego di tali SW, nonché nelle specifiche attività di trattamento dei dati a cui si applica il Codice di condotta; (c) un'approfondita conoscenza ed esperienza nello svolgimento di compiti di vigilanza e controllo. La competenza tecnica può essere dimostrata, in particolare, dal possesso di una comprovata (minimo

di tre (3) anni) esperienza nelle Attività di Sviluppo dei Software Gestionali e/o nello svolgimento dei Servizi concernenti l'impiego di tali SW, nonché nel campo della sicurezza dei dati personali e della sicurezza delle informazioni, (incluso, per esempio, le norme ISO/IEC 27001 27701, 27017, 27018, linee guida OWASP); o di un'adeguata e documentata formazione nel campo della sicurezza delle informazioni, più un minimo di due (2) anni di esperienza nella sicurezza delle informazioni. La competenza legale può essere dimostrata, in particolare, da comprovata esperienza professionale (di almeno tre (3) anni) nel campo della protezione dei dati personali ed dall'eventuale possesso di idonee certificazioni, attestazioni o altre, idonee documentazioni di tale esperienza (acquisite presso gli enti o aziende ove siano state svolte le attività lavorative o professionali), oppure da adeguata formazione giuridica sulla protezione dei dati, accompagnata da relative attestazioni, certificazioni od altre idonee documentazioni (relative alla partecipazione ad attività formative specialistiche, quali, ad esempio, master, corsi di studio e professionali, specie se risulta documentato il livello di acquisizione delle conoscenze).

3. Le attività dell'OdM, debitamente rendicontate, saranno finanziate, secondo criteri di economicità ed efficienza, da parte di ciascuno dei Produttori del Software aderenti al presente Codice di condotta secondo le quote, da pagare annualmente, stabilite sulla base del fatturato annuale (voce A1 dell'ultimo bilancio chiuso e depositato in Camera di Commercio - laddove ne sussista l'obbligo - comprensivo di tutte le linee business senza tener conto dell'eventuale consolidamento a livello di gruppo; per imprese che non hanno l'obbligo di deposito del bilancio, si fa riferimento al fatturato dichiarato a livello fiscale con la relativa dichiarazione dei redditi) di ciascun aderente, i cui valori sono deliberati annualmente dal Consiglio Generale di Assosoftware con fasce proporzionali a tale fatturato e secondo procedure che non pregiudichino l'indipendenza dell'OdM, il quale si doterà di un tariffario contenente la specificazione di tali quote in linea con quanto previsto nel regolamento dell'Organismo di cui al successivo punto 6, ultima parte, e di un manuale contenente specifiche istruzioni operative, definito d'intesa con Assosoftware, nel quale saranno dettagliate l'organizzazione e la gestione operativa ed economica dell'Organismo medesimo.

Monitoraggio del rispetto del Codice di condotta

4. Il monitoraggio del rispetto delle disposizioni del Codice di condotta da parte di ciascun Produttore del Software Gestionale per cui si è aderito al presente Codice di condotta è effettuato dall'OdM secondo una programmazione delle attività definita in base alla tipologia e alle caratteristiche dei SW Gestionali per cui si è aderito e a quanto rilevato dal medesimo Organismo nell'ambito della verifica della documentazione, del questionario di autovalutazione e della dichiarazione presentati con la domanda di adesione ai sensi dell'Allegato E del Codice di Condotta. Il monitoraggio è svolto dall'Organismo, focalizzando le attività principalmente sulla verifica del rispetto da parte del Produttore del SW delle misure tecniche, organizzative e di sicurezza di cui all'Allegato A e

all'Allegato B del Codice di condotta e dell'osservanza degli altri principi, requisiti e regole previsti dal presente Codice di condotta. Per quanto concerne gli aspetti tecnici, la verifica della conformità al Codice di condotta può essere svolta sulla base anche dei criteri previsti da norme tecniche o di standard industriali riconosciuti equivalenti, ove adottati dal Produttore del Software, che dimostrano un'adeguata attuazione dei contenuti del presente Codice di condotta.

5. Ai fini del controllo del rispetto del presente Codice di condotta da parte di tutti i Produttori ad esso aderenti, l'OdM potrà in ogni momento, anche senza necessità di preavviso, svolgere tutte le verifiche ritenute opportune, ivi incluse ispezioni, sia in remoto che presso la sede dei Produttori, i quali saranno tenuti a prestare la massima collaborazione ai fini del proficuo svolgimento di tali attività. Tali verifiche possono essere delegate dall'Organismo a collaboratori, consulenti o fornitori esterni di servizi che siano in possesso delle specifiche conoscenze e competenze in materia di protezione dei dati personali e in relazione al settore delle Attività di Sviluppo dei Software Gestionali e/o dei Servizi concernenti l'impiego di tali SW. A seguito di ciascuna verifica, l'OdM redige un verbale delle attività svolte e una relazione riepilogativa delle risultanze in merito alla conformità del Produttore del Software alle disposizioni del presente Codice di condotta e trasmette il verbale e la relazione al Produttore del Software oggetto di verifica.

6. Le procedure, modalità ed i tempi di svolgimento dell'attività di monitoraggio dell'OdM e del procedimento di verifica del rispetto delle disposizioni del presente Codice di condotta da parte dei Produttori del Software aderenti al medesimo Codice saranno definite con apposito regolamento adottato dall'OdM, sulla base dello schema predisposto da Assosoftware, ed allegato alla domanda di accreditamento presentata al Garante.

Trattazione dei reclami degli interessati

7. L'OdM sarà altresì chiamato a gestire i reclami provenienti da qualsiasi interessato in ordine a presunte violazioni del presente Codice di condotta.

8. Fatta salva la possibilità, al ricorrere dei necessari presupposti, di presentare un reclamo al Garante e/o di avviare azioni di tutela dei propri diritti in sede giudiziaria, ogni interessato che ritenga che i propri diritti siano stati lesi da uno o più trattamenti svolti da un Produttore del Software aderente al presente Codice di condotta, può proporre reclamo all'OdM, inviando al medesimo Organismo apposita istanza che dovrà contenere una breve descrizione dei fatti e del pregiudizio lamentato.

9. La presentazione di un reclamo al Garante o l'avvio di un procedimento in sede giudiziaria ordinaria o amministrativa preclude l'avvio, o determina l'improcedibilità, qualsiasi sia lo stato di svolgimento, di una procedura avente il medesimo oggetto o comunque attinente alle medesime questioni dinanzi all'OdM.

10. Entro dieci (10) giorni lavorativi dal ricevimento del reclamo l'OdM dovrà darne notizia al Produttore del Software coinvolto, affinché quest'ultimo possa, entro i successivi trenta (30) giorni lavorativi, presentare le informazioni e documentazioni necessarie o comunque utili per l'esame e valutazione del reclamo. Garantendo la pienezza del contraddittorio in ogni fase della procedura, qualora gli elementi acquisiti già consentano all'OdM di definire la procedura sul reclamo, quest'ultimo dovrà adottare la propria decisione entro quarantacinque (45) giorni lavorativi dalla data di deposito delle informazioni e documentazioni da parte del Produttore del Software. Diversamente, l'OdM potrà richiedere ad entrambe le parti ulteriori precisazioni, così come l'acquisizione di documenti o lo svolgimento di audizioni, raccogliendo in ogni caso tutti gli elementi necessari alla definizione del reclamo, che non potrà avvenire oltre novanta (90) giorni lavorativi successivi alla data di presentazione dello stesso. La procedura, le modalità ed i tempi di trattazione dei reclami da parte dell'OdM saranno definite più in dettaglio mediante il regolamento di cui al precedente punto 6, ultima parte.

Decisioni e relazioni dell'OdM

11. In conseguenza delle verifiche effettuate in esecuzione dei propri compiti di monitoraggio o di trattazione di reclami, l'OdM potrà decidere, fornendo adeguata motivazione, di applicare al Produttore del Software, in dipendenza della gravità, del numero e della reiterazione delle violazioni del Codice eventualmente riscontrate, una delle seguenti misure, secondo un criterio di gradualità e con le modalità e forme previste dal regolamento di cui al precedente punto 9:

a. un invito al Produttore del Software a modificare la condotta, in considerazione di una maggiore aderenza alle previsioni del Codice;
b. un richiamo formale indirizzato esclusivamente al Produttore del Software;
c. in caso di in caso di reiterazione della condotta rilevante di cui alle precedenti lett. a) e b), la sospensione temporanea dall'adesione al presente Codice di condotta;
d. in caso di grave e persistente inosservanza delle misure di cui alle precedenti lettere, la revoca dall'adesione al presente Codice di condotta.

12. Le decisioni mediante cui vengano applicate, a seguito di attività di verifica o della definizione di procedure di reclamo, misure di sospensione temporanea o di revoca dell'adesione della SW aderente al Codice di condotta, devono essere trasmesse al Garante, da parte dell'OdM, entro tre (3) giorni dalla loro adozione.

13. Qualora dalla decisione adottata dall'OdM, all'esito dell'attività di verifica o della definizione di una procedura di reclamo, sia derivata l'applicazione nei confronti di un Produttore del Software di misure di sospensione temporanea o di revoca dell'adesione al Codice di condotta, l'OdM, previo

oscuramento dei dati personali eventualmente presenti, provvede alla loro pubblicazione, anche in forma sintetica, in un'apposita sezione del sito web dell'OdM medesimo.

14. Alla scadenza di ciascun semestre, eccezion fatta per la revoca e la sospensione temporanea dell'adesione che dovranno essere tempestivamente comunicate al Garante, l'OdM dovrà fornire al Garante un resoconto riassuntivo dei controlli e delle verifiche effettuate, delle procedure di reclamo definite e delle misure eventualmente adottate ai sensi del comma che precede. Tale resoconto verrà inviato per opportuna informazione anche ad Assosoftware.

15. Per ogni aspetto riguardante il funzionamento e i compiti dell'OdM che non sia specificamente disciplinato dal presente Codice di condotta, si applica il Regolamento dell'OdM medesimo**.**

ALLEGATO E - MODALITÀ DI ADESIONE AL CODICE DI CONDOTTA

I Produttori di Software, anche se non associati ad Assosoftware, possono presentare domanda di adesione al presente Codice di condotta per uno o più Software Gestionali dagli stessi prodotti, laddove ritengano che tali SW soddisfino i requisiti del medesimo Codice.

A tal fine, inviano la domanda all'ufficio di Segreteria dell'OdM presso Assosoftware, secondo le modalità qui di seguito descritte.

In particolare, il Produttore presenta all'OdM la domanda di adesione redatta secondo la modulistica ed istruzioni rese disponibili sul Sito web dell'OdM, nella quale andranno indicati il o i SW gestionale/i per cui intende aderire, secondo la apposita scheda sintetica pubblicata sul medesimo Sito web.

Alla domanda va allegata la documentazione indicata nella predetta modulistica[1] e un questionario compilato dal Produttore, sulla base del modello reso disponibile dall'OdM, per la autovalutazione della conformità del SW Gestionale per cui si intende aderire ai requisiti previsti dal Codice di condotta e, in particolare, alle misure previste dai relativi Allegati A e B, nonché una dichiarazione con cui il Produttore si impegna al rispetto delle regole stabilite dal medesimo Codice di condotta secondo il modello pubblicato sul predetto Sito web.

Entro i termini indicati dall'art. 20.2 del Codice di condotta, l'OdM verifica la completezza della documentazione, le informazioni riportate nel suddetto questionario di autovalutazione, la dichiarazione di impegno e l'assenza di circostanze ostative alla candidatura all'adesione al Codice di condotta da parte del Produttore richiedente. Ove necessario, può richiedere al Produttore di fornire gli ulteriori documenti ed informazioni necessarie per completare la domanda. Accertate la regolarità della domanda di adesione, la completezza delle documentazioni presentate da parte del richiedente e la sussistenza dei requisiti, l'OdM invia al Produttore richiedente apposita comunicazione, volta a dare conferma della suddetta adesione al Codice di condotta in riferimento al o ai SW per cui è stata approvata l'adesione medesima.

A seguito della ricezione di tale conferma, i dati del Produttore aderente e dei relativi SW sono inseriti nell'Elenco dei Produttori del Software aderenti pubblicato sul Sito web dell'OdM, dandone informazione anche al Garante, affinché possa aggiornare il registro di cui all'art. 40, paragrafo 6, del Regolamento.

L'eventuale mancata conferma della adesione al Codice di condotta presentata da parte di un Produttore del Software deve essere motivata da parte dell'OdM, fermo restando che tale diniego non preclude la possibilità per il Produttore di successiva presentazione della domanda di adesione che può avvenire non prima di un anno unitamente ad una breve nota che illustri le misure adottate per superare le ragioni che avevano condotto al precedente diniego.

Qualora si verificassero modifiche o variazioni rilevanti rispetto alle informazioni e documentazioni fornite dalla SWH e valutate dall'OdM in relazione al Software Gestionale per il quale si è ottenuta l'adesione al Codice di condotta, il Produttore deve, tempestivamente, darne comunicazione all'OdM e collaborare con l'OdM per fornire le integrazioni ed aggiornamenti necessari per effettuare le relative, ulteriori valutazioni al fine di poter confermare la permanenza delle condizioni relative alla

[1] Quale, ad es., visura camerale aggiornata, ultimo bilancio approvato, certificazioni di settore e/o attestazioni di terzi indipendenti.

suddetta adesione al Codice da parte del Produttore in riferimento al o ai SW per i quali è stata ottenuta.