

# GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERA 17 ottobre 2024

Approvazione del codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale e accreditamento dell'organismo di monitoraggio. (Provvedimento n. 618). (24A06197)

(GU n.278 del 27-11-2024)

## IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

Visto il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito, «regolamento»);

Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito il «Codice») come novellato dal decreto legislativo 10 agosto 2018, n. 101 recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679»;

Visto l'art. 40 del regolamento che prevede che le associazioni e gli altri organismi rappresentanti le categorie di titolari o responsabili del trattamento possano elaborare (modificare o prorogare) codici di condotta destinati a contribuire alla corretta applicazione del regolamento in specifici settori di attività e in funzione delle particolari esigenze delle micro, piccole e medie imprese, e che tali codici devono essere approvati dall'autorità di controllo competente;

Visto il considerando 98 del regolamento che prevede che tali codici possono calibrare gli obblighi del titolare e del responsabile del trattamento, tenuto conto dei potenziali rischi del trattamento per i diritti e le libertà degli interessati;

Viste le «Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679» adottate dal Comitato europeo per la protezione di dati (di seguito «Comitato») il 4 giugno 2019, all'esito della consultazione pubblica;

Considerato in particolare che l'adesione ad un codice di condotta può essere utilizzata come elemento di responsabilizzazione (c.d. accountability), in quanto consente di dimostrare la conformità dei trattamenti di dati, posti in essere dai titolari e/o dai

responsabili del trattamento che vi aderiscano, ad alcune disposizioni o principi del regolamento, o al regolamento nel suo insieme (cfr. cons. 77 e articoli 24, par. 3, e 28, par. 5, e 32, par. 3 del regolamento);

Rilevato che il Garante incoraggia lo sviluppo di codici di condotta per le micro, piccole e medie imprese al fine di promuovere un'attuazione effettiva del regolamento, aumentare la certezza del diritto per titolari e responsabili del trattamento e rafforzare la fiducia degli interessati in ordine alla correttezza dei trattamenti di dati che li riguardano;

Rilevato che, ai sensi dell'art. 55 del regolamento e art. 2-bis del Codice, il Garante e' l'autorita' di controllo competente ad approvare i codici di condotta aventi validita' nazionale nell'esercizio del potere conferitole ai sensi dell'art. 57, paragrafo 1, lettera m) del regolamento;

Considerato che l'art. 41, par. 1, del regolamento prevede che, fatti salvi i compiti e i poteri dell'autorita' di controllo competente, la verifica dell'osservanza delle disposizioni di un codice di condotta, ai sensi dell'articolo 40 del regolamento, e' effettuata da un organismo di monitoraggio (di seguito, «Odm») in possesso dei requisiti fissati dall'art. 41, par. 2 del regolamento e del necessario accreditamento rilasciato a tal fine dalla medesima autorita', con la sola eccezione del trattamento effettuato da autorita' pubbliche e da organismi pubblici per il quale non e' necessaria l'istituzione di un Odm (art. 41, par. 6 del regolamento);

Rilevato, in questo contesto, che l'obbligo di affidare il monitoraggio dei codici di condotta a un Odm accreditato non dovrebbe costituire un ostacolo allo sviluppo di tali strumenti e che, quindi, va riconosciuto un certo margine di flessibilita' ai promotori dei codici di condotta nell'applicazione dei requisiti di accreditamento fissati dal Garante, al fine di definire il modello di Odm piu' adeguato a controllarne l'osservanza, fermo restando il rispetto di quanto previsto dal regolamento, dalle linee guida e dai pertinenti pareri del Comitato;

Considerato che il regolamento e le linee guida del Comitato sopra citate, fissano un quadro organico di riferimento per la definizione dei requisiti che l'Odm deve soddisfare per ottenere l'accreditamento;

Rilevato altresì che il Garante nella procedura di accreditamento, volta a verificare che l'Odm soddisfi i predetti requisiti, tiene in considerazione le specificita' dei trattamenti di dati personali afferenti al settore a cui si applica il codice di condotta e, in particolare, la natura e la dimensione del settore, la tipologia e il numero (anche atteso) di soggetti aderenti, la peculiarita' e la complessita' delle operazioni di trattamento oggetto del codice, nonché i rischi per gli interessati;

Considerato che l'art. 41, par. 3, del regolamento prevede che la predetta autorita' di controllo presenta al Comitato uno schema di requisiti per l'accreditamento dell'Odm, ai sensi del meccanismo di coerenza di cui all'art. 63 del regolamento;

Visto il provvedimento del 10 giugno 2020, n. 98 - pubblicato nella Gazzetta Ufficiale n. 173 dell'11 luglio 2020 - (di seguito, «Provvedimento») con il quale il Garante, ai sensi dell'art. 57, par.1, lettera p), del regolamento, ha approvato i requisiti per l'accreditamento dell'Odm, tenendo conto delle osservazioni rese dal Comitato nel parere adottato il 25 maggio 2020;

Considerato che l'art. 57, par. 1, lettera q) del regolamento prevede, in particolare, che ciascuna autorita' di controllo, sul proprio territorio, effettua l'accreditamento dell'Odm, ai sensi

dell'art. 41;

Rilevato che, ai sensi del combinato disposto di cui agli articoli 55 del regolamento e art. 2-bis del Codice, il Garante e' l'autorita' di controllo competente a definire e pubblicare i requisiti per l'accreditamento dell'Odm, nonche' ad accreditare lo stesso Odm nell'esercizio del potere conferitole ai sensi dell'art. 57, par. 1, lettere p) e q), del regolamento;

Considerato che l'Associazione proponente, Assosoftware - Associazione italiana dei produttori di software, rappresentando adeguatamente le imprese operanti in Italia nello specifico settore della produzione del software di tipo gestionale, e' legittimata, ai sensi dell'art. 40, paragrafo 2 del regolamento, a promuovere l'adozione di un codice di condotta nel settore di riferimento;

Visto che in data 30 settembre 2024, all'esito di una complessa interlocuzione con gli uffici, l'Associazione proponente ha sottoposto all'approvazione del Garante il «Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale» ed ha contestualmente presentato la richiesta formale di accreditamento dell'Odm allegando la documentazione utile idonea a comprovare il possesso dei requisiti richiesti;

Rilevato, all'esito dell'esame di questa autorita', che il codice di condotta presentato dall'Associazione proponente offre, in misura sufficiente, garanzie adeguate a tutela degli interessati nel settore di riferimento, come previsto dall'art. 40, paragrafo 5, del regolamento;

Rilevato che dall'esame della richiesta di accreditamento e della documentazione ad essa allegata, emerge che l'istituendo Odm rispetta i requisiti previsti dall'art. 41, par. 2 del regolamento e dal provvedimento, essendo stato comprovato, in particolare: un adeguato livello di competenza per lo svolgimento dei compiti di verifica sul rispetto del codice di condotta; di poter assolvere alle proprie funzioni con indipendenza e imparzialita'; di aver definito misure idonee a individuare e mitigare il rischio di eventuali conflitti di interesse;

Ritenuto, ai sensi dell'art. 57, par. 1, lettera m), del regolamento di approvare il codice di condotta che acquista la piena efficacia dal giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana e sara' inserito nei registri di cui all'art. 40, parr. 6 e 11 del regolamento;

Ritenuto, pertanto, ai sensi dell'art. 57, par. 1, lettera q), del regolamento, di accreditare l'Odm individuato dal proponente alla verifica del rispetto del codice di condotta, per la durata di cinque anni non rinnovabili;

Vista la documentazione in atti;

Viste le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Pasquale Stanzone;

Tutto cio' premesso il Garante

a) ai sensi dell'art. 57, par. 1, lettera m), del regolamento approva il codice di condotta riportato in allegato al presente provvedimento del quale forma parte integrante;

b) ai sensi dell'art. 57, par. 1, lettera q), del regolamento accredita l'Odm proposto dal proponente alla verifica del rispetto del codice di condotta per la durata di cinque anni non rinnovabili;

c) invia copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini

della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 17 ottobre 2024

Il Presidente e relatore: Stanzione

Il Segretario generale: Mattei

Allegato

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

## INDICE

### PREAMBOLO

Articolo 1 - Ambito di applicazione  
Articolo 2 - Definizioni  
Articolo 3 - Progettazione e sviluppo di SW Gestionali: Privacy by design e by default  
Articolo 4 - Installazione, assistenza e manutenzione del SW Gestionale  
Articolo 5 - Ruolo della SWH quale responsabile del trattamento: garanzie, obblighi e responsabilit   
Articolo 6 - Accordo sul trattamento dei dati personali con il cliente  
Articolo 7 - Ricorso della SWH a sub-responsabili del trattamento  
Articolo 8 - Trattamenti per i quali la SWH agisce in qualita' di titolare del trattamento  
Articolo 9 - Registri dei trattamenti della SWH quale responsabile del trattamento  
Articolo 10 - Analisi dei rischi e valutazione d'impatto sulla protezione dati  
Articolo 11 - Misure adottate per la sicurezza del trattamento dei dati personali  
Articolo 12 - Gestione degli incidenti di sicurezza  
Articolo 13 - Persone autorizzate operanti sotto il controllo della Software House  
Articolo 14 - Assistenza al cliente nella gestione delle richieste per l'esercizio dei diritti degli interessati  
Articolo 15 - Trasferimento dei dati in Paesi terzi al di fuori della UE  
Articolo 16 - Tempi di conservazione dei dati: cancellazione o restituzione dei dati al cliente  
Articolo 17 - Richieste di informazioni e controlli del cliente  
Articolo 18 - Cooperazione con le Autorita' di controllo, con l'Autorita' giudiziaria e di polizia giudiziaria e tributaria  
Articolo 19 - Verifiche sul rispetto del codice di condotta ed Organismo di monitoraggio  
Articolo 20 - Modalita' 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 Attivit  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: Modalita' 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 e' 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 competitivita' 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 attivita' 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 attivita' contabilita', 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 conformita' degli operatori piu' 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 necessita' 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'obiettivo di rendere disponibili ai clienti, operanti quali Titolari o responsabili del trattamento, idonei strumenti e funzionalita' 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 conformita' 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 piu' prodotti dagli stessi sviluppati sono volte quindi a promuovere tra i clienti richiedenti ed utilizzatori di Software Gestionali:

i. la conformita' 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 attivita' di trattamento di dati personali.

6. Il presente codice ha ad oggetto non solo le attivita' di progettazione e sviluppo dei Software, che di regola non comportano il trattamento di dati personali, ma anche le attivita' 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.: attivita' di migrazione dati finalizzata all'installazione del Software, attivita' di assistenza e aggiornamento SW con accesso da remoto, acquisizione o esportazione di copia di dati per verifica di problematiche tecniche, ecc.). Queste ultime attivita' possono essere svolte in diversi contesti: (i) on premise, ossia quando il Software e' 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 responsabilita' del cliente, quale titolare del trattamento o responsabile. Il presente codice di condotta non ha ad oggetto e non intende pertanto disciplinare le attivita' di trattamento di dati personali eventualmente 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 contabilita',

fatturazione, ecc.).

Art. 1.  
Ambito di applicazione

1.1. Il presente codice di condotta e' riferito alle attivita' 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 e' applicabile unicamente a livello nazionale. Per tale motivo, l'approvazione di cui all'art. 40 del regolamento e' richiesta al Garante in qualita' di Autorita' di controllo competente ai sensi dell'art. 55 del regolamento.

1.2. Il presente codice di condotta e' 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 e' applicabile nei riguardi dei trattamenti di dati personali connessi allo svolgimento da parte della Software House di attivita' secondarie o comunque non riguardanti la produzione del software gestionale, che sono comuni e trasversali rispetto alla generalita' 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.).

Art. 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 attivita';

c) servizi: i servizi relativi alle attivita' di installazione, messa in esercizio, assistenza, manutenzione, gestione, aggiornamento del software gestionale prodotto dalla SWH;

d) Attivita' di Sviluppo: le attivita' di progettazione, sviluppo e produzione del software gestionale, che non comportano di regola lo svolgimento di attivita' di trattamento di dati personali;

e) clienti: i soggetti che richiedono ai Produttori lo sviluppo ed installazione dei Software Gestionali e le connesse attivita' 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.

Art. 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.

#### Art. 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, puo' rivestire tale ruolo solo qualora venga chiamato a svolgere attivita' 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) attivita' di migrazione dati finalizzata all'installazione e al collaudo del software gestionale;

b) attivita' di assistenza e aggiornamento del software gestionale con possibilita' (ancorche' occasionalmente) di accesso remoto ai dati del cliente (es. tramite strumenti di help-desk remoto VPN, ecc.);

c) attivita' di acquisizione di data base del cliente o esportazione e copia di dati personali del cliente per verificare problematiche di carattere tecnico e svolgere attivita' 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 trattamento, 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 attivita' di assistenza e manutenzione che comporta l'accesso ad infrastrutture e sistemi del cliente su cui e' 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 attivita' e gli obblighi del produttore quale responsabile del trattamento non si estendono alle attivita' di gestione e manutenzione dell'infrastruttura su cui e' installato il software gestionale, la cui responsabilita' resta a carico del cliente. In particolare, restano escluse, nei contesti on premise, dalla responsabilita' del produttore del software, le attivita' di salvataggio e ripristino dei dati personali cosi' come tutte le attivita' necessarie alla protezione della sicurezza fisica e logica dell'infrastruttura su cui il Software e' installato.

#### Art. 5.

Ruolo della SWH quale responsabile del trattamento: garanzie, obblighi e responsabilita'

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 possibilita' 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 liceita' delle attivita' di trattamento dei dati svolte per conto del cliente. Resta ferma la possibilita' per il produttore del software di rifiutarsi di eseguire attivita' di trattamento dei dati che risultino palesemente in contrasto con la vigente normativa in materia di protezione dei dati personali, dandone evidenza al cliente.

## Art. 6.

## Accordo sul trattamento dei dati personali con il cliente

6.1. Nei casi previsti ai precedenti articoli 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.

## Art. 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 puo' 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 puo' 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 puo' 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 puo' 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.

#### Art. 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 attivita' di help-desk a supporto degli Utenti del cliente, ecc.). Per le attivita' di trattamento dei dati personali svolte in qualita' di titolare del trattamento, il produttore del software e' 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, puo' 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 funzionalita') esclusivamente in forma aggregata, mediante il calcolo di opportune metriche e indicatori, per il perseguimento di legittimi interessi correlati a finalita' statistiche, di analisi, studio e ricerca volte a migliorare la sicurezza, le prestazioni e le funzionalita' dei medesimi Software e dei connessi servizi, a beneficio anche degli stessi clienti che ne fruiscono. Per tali finalita', l'elaborazione dei predetti dati personali e' effettuata dal produttore del software previa adozione di tecniche di pseudonimizzazione o cifratura dei dati in modo tale da limitare la diretta riconducibilita' delle informazioni agli Interessati, nonche' sulla base della preventiva informativa fornita agli interessati circa le suddette finalita' del trattamento e i legittimi interessi perseguiti.

8.3. Per le finalita' sopra indicate l'informativa agli interessati puo' 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 funzionalita', che possono rinviare ad un'informativa piu' 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.

#### Art. 9.

Registri dei trattamenti della SWH quale responsabile del trattamento

9.1. Il produttore del software che agisce quale responsabile del trattamento e' tenuto a mantenere un registro delle attivita' 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 attivita' di responsabili del trattamento in favore di un elevato numero di clienti quali Titolari, nella tenuta e conservazione dei Registro delle attivita' di trattamento possono essere adottate le seguenti modalita':

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 puo' 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.

#### Art. 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, e' altresì volta a facilitare i clienti nelle valutazioni condotte ex articoli 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 articoli 24, 25, 35 e 36 del regolamento.

#### Art. 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.

#### Art. 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 dieci 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 articoli 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 articoli 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 articoli 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 articoli 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 qualita' 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 e' 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, affinche' lo stesso possa estrarne o chiederne copia secondo le modalita' convenute con il produttore del software.

16.3. Il produttore del software ha la facolta' 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 necessita' esplicita, legittima e trasparente del medesimo produttore (es. finalita' 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 attivita' 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 modalita' 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 conformita' 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 puo' 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 puo' 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 conformita' 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 verterà 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 gestionali 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 presentata dal produttore e (ii) della sussistenza dei requisiti di

conformita' 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, nonche' (iii) dell'assenza di condizioni ostative all'adesione da parte del produttore richiedente. Ove necessario, l'Organismo puo' 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 attivita' 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 e' stata richiesta e, contestualmente, a comunicare la nuova adesione al Garante, affinche' 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 e' 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 attivita' 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 dovra' essere motivata da parte dell'OdM, fermo restando che tale diniego non preclude il successivo rinnovo della domanda di adesione che potra' 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 cio' 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, puo' in ogni momento promuovere il riesame del presente codice di condotta e dei relativi allegati, anche alla luce di novita' 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, e' pubblicato nella Gazzetta Ufficiale della Repubblica Italiana ed acquista efficacia il giorno successivo a quello della pubblicazione.

(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

## Allegato A

Parte di provvedimento in formato grafico

## Allegato B

Parte di provvedimento in formato grafico

## Allegato C

Parte di provvedimento in formato grafico

## Allegato D

## Organismo di monitoraggio

1. L'OdM e' 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'«Autorita'») ai sensi dell'art. 41 del regolamento (UE) 2016/679. L'OdM e' 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 onorabilita', indipendenza, imparzialita', conflitto di interessi e competenza sotto indicati per i componenti degli OdM. L'OdM sara' 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 svolgera' funzioni di supervisione e cura del coordinamento e dell'organizzazione delle attivita' dell'Organismo medesimo.

L'incarico dei componenti dell'OdM, avra' la durata di cinque (5) anni, non rinnovabile. Prima della scadenza del mandato dell'OdM, Assosoftware provvedera' a richiedere l'accreditamento dell'organismo nella nuova composizione. Per le relative attivita' amministrative e di segreteria, l'OdM puo' avvalersi del supporto di personale reclutato tramite agenzie esterne di lavoro e/o messo a disposizione da Assosoftware, purché esclusivamente dedicato alle attivita' 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 necessita' di personale di supporto, il relativo incarico potra' 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 decreto legislativo 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 puo' essere dimostrata, in particolare, dal possesso di una comprovata (minimo di tre (3) anni) esperienza nelle attivita' di sviluppo dei software gestionali e/o nello svolgimento dei Servizi concernenti l'impiego di tali SW, nonche' 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, piu' un minimo di due (2) anni di esperienza nella sicurezza delle informazioni. La competenza legale puo' 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 attivita' 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 attivita' formative specialistiche, quali, ad esempio, master, corsi di studio e professionali, specie se risulta documentato il livello di acquisizione delle conoscenze).

3. Le attivita' dell'OdM, debitamente rendicontate, saranno finanziate, secondo criteri di economicita' 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 dotera' 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 e' aderito al presente codice di condotta e' effettuato dall'OdM secondo una programmazione delle attivita' definita in base alla tipologia e alle caratteristiche dei SW Gestionali per cui si e' 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 e' svolto dall'Organismo, focalizzando le attivita' 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 conformita' al codice di condotta puo' 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 potra' in ogni momento, anche senza necessita' 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 attivita'. 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 attivita' 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 attivita' svolte e una relazione riepilogativa delle risultanze in merito alla conformita' 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, modalita' ed i tempi di svolgimento dell'attivita' 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 sara' altresì chiamato a gestire i reclami provenienti da qualsiasi interessato in ordine a presunte violazioni del presente codice di condotta.

8. Fatta salva la possibilita', 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 piu' trattamenti svolti da un produttore del software aderente al presente codice di condotta, puo' proporre reclamo all'OdM, inviando al medesimo Organismo apposita istanza che dovra' 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'improcedibilita', 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 dovra' darne notizia al produttore del software coinvolto, affinche' 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 gia' consentano all'OdM di definire la procedura sul reclamo, quest'ultimo dovra' 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 lettere 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 sicurezza



I Produttori di Software, anche se non associati ad Assosoftware, possono presentare domanda di adesione al presente Codice di condotta per uno o piu' 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 modalita' 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 (2) e un questionario compilato dal produttore, sulla base del modello reso disponibile dall'OdM, per la autovalutazione della conformita' 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, nonche' 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, puo' richiedere al produttore di fornire gli ulteriori documenti ed informazioni necessarie per completare la domanda. Accertate la regolarita' 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 e' 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, affinche' 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 possibilita' per il produttore di successiva presentazione della domanda di adesione che puo' 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 e' 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 suddetta adesione al Codice da parte del produttore in riferimento al o ai SW per i quali e' stata ottenuta.

(2) Quale, ad es., visura camerale aggiornata, ultimo bilancio

approvato, certificazioni di settore e/o attestazioni di terzi  
indipendenti.