Procedura relativa all'esecuzione di attività di controllo e monitoraggio nei confronti dei Produttori aderenti

1. Finalità e struttura della Procedura

La presente Procedura (di seguito, la '**Procedura**'), basata su uno schema proposto dall'Associazione Italiana Produttori Software (di seguito "**Assosoftware**") - in linea con i documenti pubblicati da organismi di monitoraggio di altri codici di condotta precedentemente adottati in Italia - , stabilisce le regole e le procedure applicabili allo svolgimento di controlli e verifiche da parte dell'Organismo di monitoraggio (di seguito, l''**OdM**' o l''**Organismo**') costituito, ai sensi dell'articolo 41 del Regolamento (UE) 2016/679 (di seguito, il '**GDPR**'), al fine di garantire il rispetto del 'Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale' approvato dal Garante per la protezione dei dati personali con il provvedimento n. 618 del 17 ottobre 2024 (di seguito, il '**Codice di Condotta**').

Al fine di dare attuazione e garantire il rispetto di quanto previsto dal Codice di Condotta e dal Regolamento interno sul funzionamento dell'organismo di monitoraggio del 'Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale' (di seguito, il '**Regolamento interno**'), adottato in data 23 maggio 2025, l'OdM ha ritenuto opportuno redigere il presente documento al fine di:

1. definire il metodo e l'iter di svolgimento delle attività di controllo e verifica previste dal Codice di Condotta nei confronti dei Produttori ad esso aderenti, siano essi associati o meno a Assosoftware;
2. identificare puntualmente le diverse fasi del procedimento e, per ciascuna di esse, le specifiche attività da espletarsi;
3. dotarsi di uno strumento operativo in grado di favorire la corretta attuazione di quanto previsto dal Codice di Condotta e dal Regolamento interno.

La funzione di monitoraggio e controllo attribuita all'Organismo dal Codice di Condotta si esplica, oltre che nella gestione dei reclami che possono insorgere fra i Produttori e gli Interessati, per cui è stata adottata una distinta, specifica Procedura, in particolare nello svolgimento di attività di verifica del concreto e costante rispetto, da parte dei Produttori, di tutte le prescrizioni del Codice di Condotta e, più in generale, della normativa applicabile in materia di protezione dei dati personali.

La rilevanza pubblica di alcune delle decisioni che possono essere assunte all'esito delle attività di verifica, così come gli obblighi informativi nei confronti del Garante, rendono ancora più evidente l'importanza di disporre di strumenti, come questa Procedura, utili ad assicurare il rispetto di quanto previsto dal Codice di Condotta e dal Regolamento interno.

Tramite questo documento si intendono quindi stabilire, in maniera chiara e puntuale, le regole connesse all'esecuzione delle procedure di verifica, che l'OdM è tenuto a svolgere ai sensi dell'articolo 19 e dei paragrafi 4, 5 e 6 dell'Allegato D del Codice di Condotta, nonché dell'art. 7 del Regolamento interno.

In merito alla struttura della presente Procedura, dopo averne circoscritto il campo di applicazione ed aver delineato alcune definizioni basilari, si fornirà una descrizione della metodologia e delle fasi del procedimento di verifica e controllo previsto nei confronti dei Fornitori.

2. Ambito di applicazione della Procedura

Il perimetro applicativo del presente documento deve essere definito sia in riferimento alla natura delle attività in esso disciplinate (ambito oggettivo), sia alle categorie di soggetti che ne sono destinatari (ambito soggettivo).

2.1 Ambito oggettivo

La Procedura si applica a qualsiasi attività di controllo svolta da parte dell'Organismo, a prescindere dalla forma di volta in volta prescelta (es. verifica in loco, richieste scritte di informazioni e documenti) per verificare la corretta attuazione del Codice di Condotta ed il puntuale adempimento di tutti gli obblighi stabiliti dalla normativa vigente in materia di protezione dei dati personali da parte dei Produttori.

2.2 Ambito soggettivo

I soggetti destinatari cui deve applicarsi questa Procedura sono:

- i Componenti dell'Organismo, attuali e futuri, chiamati ad eseguire i controlli richiesti dal Codice di Condotta e dal Regolamento interno;
- i Produttori oggetto di verifica ai sensi del Codice di Condotta;
- gli eventuali Fornitori a cui siano delegate attività di controllo oggetto della presente Procedura, per conto e su incarico specifico dell'OdM;
- il personale amministrativo della Fondazione, incluso il Segretario, operante in favore dell'Organismo, qualora coinvolto in alcuna delle attività descritte nella presente Procedura.

(di seguito, congiuntamente, i '**Destinatari'**).

3. Definizioni

Ai fini della presente Procedura si applicano le definizioni previste dall'art. 4 del Regolamento UE 679/2016 e dall'art. 2 del Codice. Ai medesimi fini si applicano anche le ulteriori definizioni di seguito riportate:

- **Componenti**: i tre membri dell'Organismo designati secondo le regole dettate dal Codice di Condotta (Allegato D) e dal Regolamento interno;
- **Contratto**: si intende qualsiasi rapporto contrattuale concluso dalla Fondazione, su proposta dell'Organismo, mediante sottoscrizione di apposito contratto o accordo con un Fornitore;

- **Fondazione**: la Fondazione per la Promozione e il Monitoraggio del Codice di Condotta dei Produttori di Software ETS, all'interno della quale opera in piena autonomia e indipendenza anche finanziaria, l'OdM;

- **Fornitore/i**: qualsiasi soggetto terzo (collaboratore, consulente o fornitore) rispetto all'organizzazione dell'Organismo, della Fondazione, di Assosoftware o di qualsiasi Produttore, con cui la Fondazione su proposta dell'OdM concluda un Contratto avente ad oggetto la delega o affidamento di specifiche attività di controllo e monitoraggio, ad eccezione di quelle che presuppongono o determinano l'esercizio di poteri decisionali del medesimo Organismo.

4. Fonti di riferimento

Oltre che sul Codice di Condotta e sul Regolamento interno, la presente Procedura è basata, inter alia, sulle seguenti fonti:

- il Regolamento (UE) 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;
- il D.lgs. 30 giugno 2003, n. 196, recante il 'Codice in materia di protezione dei dati personali', come modificato ed integrato dal D.lgs. 10 agosto 2018, n. 101, recante 'Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679' (di seguito, il 'Codice Privacy');
- le Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del Regolamento generale sulla protezione dei dati, adottate in via definitiva dall'EDPB il 4 giugno 2019;
- le Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del Regolamento (UE) 2016/679, adottate dall'EDPB il 4 giugno 2019;
- il provvedimento n. 98 del 10 giugno 2020, con il quale il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera p), del Regolamento, ha approvato i requisiti per l'accreditamento dell'OdM, tenendo conto delle osservazioni rese dall'EDPB nel parere adottato il 25 maggio 2020;
- il provvedimento n. 618 del 17 ottobre 2024, con il quale il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera q) del Regolamento, all'esito dell'esame della richiesta di accreditamento e della relativa documentazione presentata da Assosoftware il 30 settembre 2024, ha accreditato l'OdM preposto alla verifica del rispetto del Codice di Condotta.

5. Attività di controllo

Fermo restando il potere dell'OdM di svolgere, in qualsiasi momento e senza necessità di preavviso, tutte le verifiche di volta in volta ritenute opportune per accertare il pieno rispetto, da parte dei

Produttori aderenti, degli obblighi stabiliti dal Codice di Condotta, le attività di controllo avverranno in particolare nei seguenti casi (di seguito, i '**Controlli Saltuari**):

- sulla base della rilevazione di una o più violazioni della normativa applicabile;
- sulla base del consistente numero di reclami ricevuti da parte degli Interessati.

A prescindere da quanto sopra e quindi eventualmente in aggiunta ai Controlli Saltuari scaturiti dalle circostanze sopra descritte, l'Organismo svolgerà attività di controllo o monitoraggio (di seguito "**Controlli Programmati**") sulla base di un calendario o programma di attività predisposto a cura dell'OdM stesso e previamente condiviso con ciascun Produttore interessato dalle programmate attività di controllo, tenuto conto della tipologia e delle caratteristiche del/i SW Gestionale/i per cui si è aderito al Codice di condotta, nonché di quanto rilevato nell'ambito della verifica della documentazione, del questionario e della dichiarazione presentati con la domanda di adesione ai sensi dell'Allegato E del Codice di Condotta.

Ciascuna attività di Controllo Programmato è svolta 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 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 Codice di condotta.

6. Tipologia di controlli eseguibili

In conformità a quanto stabilito dal Codice di Condotta (Allegato D), l'Organismo può assolvere ai propri compiti di controllo e monitoraggio eseguendo tutte le verifiche ritenute necessarie ed opportune per accertare il puntuale rispetto, da parte del Produttore coinvolto, delle regole del Codice di Condotta e delle misure di cui ai relativi Allegati A e B.

Tali verifiche possono essere svolte, anche in ragione dei profili che l'OdM intende specificamente controllare, mediante gli strumenti di consultazione e di controllo che quest'ultimo considera più idonei al raggiungimento degli obiettivi di volta in volta identificati, previa adozione da parte dell'Organismo di adeguate misure volte a garantire al riservatezza e sicurezza delle informazioni e documentazioni acquisite da ciascun Produttore nell'ambito delle verifiche e dei controlli di cui alla presente Procedura.

L'OdM può quindi esercitare tutti i poteri di verifica necessari ad assicurare una puntuale ed efficiente vigilanza sull'osservanza del Codice di Condotta, tra cui a titolo esemplificativo:

- inviare richieste scritte di informazioni e documenti;
- chiedere la compilazione di appositi questionari o check list;

- eseguire attività di verifica (c.d. audit) sia in remoto, che *in loco* presso cioè la sede o i locali aziendali della SWH, ove ritenute necessarie od opportune ai fini del corretto espletamento dei propri compiti di controllo e monitoraggio, con possibilità di accesso in via collaborativa agli archivi, documenti, infrastrutture, impianti e sistemi del Produttore, al fine di ottenere ogni informazione, dato o evidenza documentale ritenuta necessaria;
- disporre, ove occorra, l'audizione di dipendenti, amministratori e dirigenti del Produttore, al fine di raccogliere informazioni o chiarimenti utili, concordando preventivamente gli impegni, sempre che non vi ostino ragioni d'urgenza.

Fermo quanto sopra, le attività di controllo sono di norma eseguite da parte dell'OdM da remoto, anche mediante sottoposizione al Produttore, di una check-list contenente almeno gli elementi di cui al questionario di autovalutazione e successivo invio, da parte del Produttore, della check-list compilata, nonché di tutta la documentazione richiesta o, in aggiunta, comunque ritenuta utile a dimostrare, in relazione al/i SW Gestionale/i per cui si aderito, piena conformità alle disposizioni del Codice di Condotta dei trattamenti e agli standard e misure di cui agli Allegati A e B. Tra la documentazione oggetto di verifica, l'OdM può richiedere anche ogni genere di evidenza informatica rilevante, quali a titolo meramente esemplificativo, estratti o copie di schermate video rilevanti, file di log e metadati, ticket di accesso a sistemi e database.

Come stabilito dal Codice di Condotta, l'Organismo può anche svolgere ispezioni presso la sede, gli uffici ed i locali rilevanti (es. CED e data center) dei Produttori, o dei loro ulteriori responsabili o sub-responsabili del trattamento, al verificarsi delle circostanze che richiedono l'esecuzione di Controlli occasionali ai sensi del precedente paragrafo 5, o in caso di gravi mancanze o acclarate criticità emerse dalla checklist o dalla successiva analisi documentale.

7. Modalità e fasi di esecuzione dei controlli

L'esecuzione di attività di controllo da parte dell'OdM richiede un preavviso nei confronti del Produttore non superiore alle 48 ore dall'invio della checklist, da parte dell'OdM, o della richiesta di informazioni o di chiarimenti, o di qualsiasi altra documentazione rilevante, oppure dell'inizio dello svolgimento di una verifica o audit in loco.

I Produttori sono tenuti a prestare la massima collaborazione nei confronti dell'OdM, o dei soggetti terzi (Fornitori) da esso appositamente delegati, ai fini del proficuo svolgimento di tutte le attività di controllo di cui al precedente paragrafo 6. L'eventuale mancato adempimento di tale obbligo deve essere valutato da parte dell'Organismo, insieme ad ogni altro elemento utile, in sede di decisione finale, all'esito delle attività di controllo, sul livello di conformità del Produttore al Codice di Condotta.

In conformità a quanto previsto dall'articolo 12, comma 2, del Codice di Condotta e nel rispetto dei requisiti stabiliti dall'articolo 6 del Regolamento interno, l'OdM può affidare l'esecuzione di attività di controllo e verifica (ad eccezione di quelle che presuppongono o determinano l'esercizio di poteri decisionali) a collaboratori, consulenti o fornitori esterni di servizi (Fornitori) 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 (v. l'apposita Procedura sulla loro selezione). Gli obblighi di cooperazione applicabili al Fornitore, descritti al paragrafo che precede, restano ovviamente immutati in tutte le ipotesi di controlli svolti da parte di Fornitori su incarico e per conto dell'Organismo.

Tutte le attività di monitoraggio e controllo svolte da parte dell'OdM ai sensi del Codice di Condotta ed in conformità alla presente Procedura devono essere documentate in apposito verbale, da inviarsi, insieme ad una relazione riepilogativa delle risultanze della verifica, al Produttore entro dieci giorni dalla chiusura delle relative operazioni. I rilievi eventualmente formulati nei confronti del Produttore sono motivati e circostanziati nella suddetta relazione riepilogativa, così che quest'ultimo possa, nei 30 giorni lavorativi successivi, fornire chiarimenti, indicazioni, documenti ed altri elementi necessari o comunque utili ai fini del superamento degli eventuali rilievi e della regolarizzazione delle eventuali carenze segnalate dall'Organismo rispetto ai requisiti, principi ed obblighi previsti dal Codice di condotta.

L'OdM potrà richiedere al Produttore ulteriori informazioni e precisazioni, così come l'acquisizione di altri documenti o lo svolgimento di audizioni, raccogliendo in ogni caso tutti gli elementi necessari alla miglior definizione del procedimento. Una volta acquisiti tutti gli elementi necessari o comunque utili per completare le relative valutazioni, l'OdM adotterà la propria decisione entro i trenta giorni lavorativi successivi dall'ultima richiesta di informazioni inviata al Produttore.

Nel caso in cui venga disposta un'audizione, di cui deve essere redatto un sintetico verbale da inviare al Produttore entro i 5 (cinque) giorni successivi, la stessa avrà luogo da remoto o presso la sede dell'Organismo nella data fissata da quest'ultimo. In sede di audizione il Produttore potrà farsi assistere anche da un avvocato o da altro consulente esterno.

La decisione finale da parte dell'Organismo, all'esito del procedimento di valutazione dei risultati delle attività di controllo e verifica, secondo quanto stabilito al successivo paragrafo 8, non potrà essere assunta oltre 90 (novanta) giorni lavorativi successivi alla data di conclusione delle stesse, come riportata sull'apposito verbale.

8. Decisioni derivanti dai controlli

Al termine della procedura descritta al precedente paragrafo 7, l'OdM può deliberare l'esito positivo della verifica (con o senza formulazione di eventuali raccomandazioni), dandone comunicazione al Produttore, oppure può decidere, fornendo adeguata motivazione, di applicare nei confronti del Produttore del Software, in dipendenza della gravità, del numero e della reiterazione delle non conformità o violazioni del Codice eventualmente riscontrate, una delle seguenti misure, secondo un criterio di gradualità:

a) un invito al Produttore Aderente del Software a modificare la condotta o regolarizzare la potenziale non conformità rilevata entro trenta (30) giorni lavorativi, al fine di garantire una maggiore aderenza alle previsioni del Codice;
b) un richiamo formale indirizzato esclusivamente al Produttore Aderente;

c) in caso di reiterazione della condotta o non conformità rilevata di cui alle precedenti lett. a. e b., la sospensione temporanea dall'adesione al presente Codice di condotta e dell'uso del relativo sigillo;
d) in caso di grave e persistente inosservanza delle misure di cui alle precedenti lettere, la revoca dall'adesione al presente Codice di condotta e dell'uso del relativo sigillo.

Le decisioni mediante cui vengano applicate misure di sospensione temporanea o di revoca dell'adesione della SW aderente al Codice di condotta, devono essere trasmesse al Garante entro tre giorni dalla loro adozione.

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.

9. Vigenza e modifiche alla presente Procedura

La presente Procedura è valida e vincolante per tutti i Destinatari.

Una copia di questo documento verrà messa a disposizione di ciascun Destinatario tramite Posta Elettronica Certificata e sarà pubblicata, sempre a cura del Segretario, sul sito web dell'Organismo.

La presente Procedura potrà essere modificata, integrata o integralmente sostituita in ogni momento, previa approvazione da parte della maggioranza dei Componenti, per garantire i necessari adeguamenti a nuove norme di legge e/o a provvedimenti dell'Autorità, oltre che alle migliori best practices di settore.

Tutti i Destinatari sono tenuti a prenderne visione e a tenere in debita considerazione gli aggiornamenti che verranno apportati alla stessa, come di volta in volta notificati. Nessun Destinatario potrà giustificare la propria condotta adducendo la mancata conoscenza della presente Procedura.