Procedura relativa alla selezione dei Fornitori da parte dell'Organismo di Monitoraggio

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 alla selezione e alla gestione dei fornitori esterni 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**' o il '**Regolamento**'), 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**'), da parte dei Produttori allo stesso aderenti.

Conformemente a quanto stabilito dall'art. 5 del *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 definire quali azioni sia necessario intraprendere ogniqualvolta sia necessario avvalersi di fornitori esterni nell'espletamento dei compiti di controllo e monitoraggio attribuiti all'OdM.

L'OdM è chiamato infatti a prestare particolare attenzione alla selezione dei collaboratori, consulenti o fornitori esterni a cui intenda delegare specifiche attività connesse ai compiti di controllo e monitoraggio attribuiti all'Organismo medesimo ai sensi del Codice di Condotta, con riferimento anche ai trattamenti di dati personali posti in essere nell'ambito dei Servizi erogati dai Produttori aderenti per uno o più Software Gestionali dagli stessi prodotti.

La presente Procedura offre, dunque, un primo strumento di verifica ed analisi utile per supportare l'OdM nella individuazione dei Fornitori e per garantire che l'affidamento di incarichi esterni, effettuato dalla Fondazione su proposta dello stesso Organismo, avvenga solamente nei confronti di collaboratori, consulenti e/o fornitori esterni che assicurino esperienza ed affidabilità elevate per eseguire con puntualità e competenza le attività delegate, nel rispetto dei principi sanciti dalla normativa in materia di protezione dei dati personali e del Codice di Condotta.

In merito alla struttura della presente Procedura, si evidenzia che verranno fornite indicazioni sugli strumenti per identificare il possibile ruolo dei Fornitori (come di seguito definiti) rispetto ai servizi esternalizzati che implichino un trattamento dei dati personali, conformemente al quadro normativo di riferimento. A seguire si introdurranno gli strumenti per garantire, su base continuativa, il mantenimento dei requisiti di garanzia e affidabilità previsti dal GDPR, dal Codice di Condotta, nonché dal Regolamento interno.

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 destinatari interessati (ambito soggettivo).

2.1 Ambito oggettivo

La presente Procedura si applica al processo di selezione dei Fornitori cui l'Organismo può delegare lo svolgimento di una o più attività di controllo e monitoraggio di cui al Codice di Condotta, ad eccezione di quelle che determinano o presuppongono l'esercizio di poteri decisionali, tenuto conto anche dei casi in cui da tali attività derivi l'esigenza per i Fornitori selezionati di trattare informazioni riservate e dati personali per conto dell'OdM in conformità alla normativa in materia di protezione dei dati personali, con particolare ma non limitato riferimento al Codice di Condotta, oltre che al Regolamento interno.

2.2 Ambito soggettivo

I soggetti destinatari cui deve applicarsi la presente Procedura sono:

- i Componenti dell'Organismo, attuali e futuri, chiamati a selezionare i Fornitori cui siano delegate attività attinenti ai relativi compiti di controllo e monitoraggio, come previsto dal Codice di Condotta e dal Regolamento interno;
- la Fondazione chiamata a concludere i contratti di servizi con tali Fornitori e il personale amministrativo (incluso il Segretario) operante in favore dell'OdM, presso la sede della medesima Fondazione e/o dell'Organismo, qualora coinvolto in una o più delle attività descritte nella presente Procedura;
- i Fornitori a cui siano delegate da parte dell'OdM attività attinenti ai relativi compiti di controllo e monitoraggio, ai sensi della vigente normativa in materia e del Codice di Condotta e del Regolamento interno;

(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 e dal Regolamento interno;
- **Contratto:** si intende qualsiasi rapporto contrattuale concluso dalla Fondazione su proposta dell'OdM 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 rispetto all'organizzazione dell'Organismo, della Fondazione, dell'Associazione Italiana Produttori Software (di seguito, '**Assosoftware**') o di un Produttore, a cui venga affidato, mediante Contratto, da parte della Fondazione su proposta dell'OdM lo svolgimento di specifiche attività di controllo e verifica del medesimo Organismo, ad eccezione di quelle che presuppongono o determinano l'esercizio di poteri decisionali dell'Organismo.

4. Fonti di riferimento

Oltre che sul Codice di Condotta e sul Regolamento interno, la presente Procedura sono basate, *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. Valutazione dei requisiti richiesti dal Regolamento interno

In relazione alle attività di controllo e monitoraggio che potranno essere delegate dall'OdM, il Fornitore è comunque tenuto ad uniformarsi a quanto previsto dal Regolamento interno, nonché dalla presente Procedura e delle ulteriori indicazioni e istruzioni fornite dall'Organismo.

In particolare, conformemente a quanto indicato negli articoli 5.3 e ss. del Regolamento interno, il Fornitore dovrà:

1. garantire il possesso, anche da parte del personale coinvolto nelle attività delegate dall'OdM, delle adeguate 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, come definiti all'art. 2.2., lettere c) e d), del Codice di condotta, nonché dell'esperienza e dell'affidabilità richieste per eseguire con puntualità le attività delegate.

2. assumersi obblighi di indipendenza ed imparzialità, trasparenza operativa, assenza di conflitti di interesse e garantire esperienza in materia di SW Gestionali, con particolare riguardo ai profili di protezione dei dati personali;

3. garantire la massima riservatezza riguardo alle notizie e/o alle informazioni di cui viene a conoscenza nel corso dell'esecuzione dell'incarico affidatogli da parte dell'Organismo;

4. fornire, al termine del suo incarico e comunque alla fine di ogni anno solare, un resoconto scritto di tutte le operazioni svolte in favore dell'OdM.

Al fine di vincolare adeguatamente il Fornitore al rispetto delle istruzioni e delle misure qui sopra identificate, l'OdM e/o la Fondazione dovranno inviare, prima di concludere le pratiche connesse all'affidamento dell'incarico – ossia prima della sottoscrizione del Contratto (e dell'eventuale DPA *ex* art. 28 GDPR) – e ricevere sottoscritta da parte del Fornitore, un'apposita dichiarazione di accettazione.

6. Il ruolo privacy del Fornitore

6.1 Qualificazione del Fornitore come Responsabile del trattamento

Nel caso in cui le attività di controllo e monitoraggio affidate dal Fornitore su proposta dell'OdM comportino il trattamento di dati personali per conto del medesimo Organismo, il medesimo Fornitore riveste il ruolo di Responsabile del trattamento ai sensi del GDPR.

6.2 Scelta del Responsabile del trattamento

Tenuto conto di quanto stabilito dall'articolo 28 del GDPR, occorre valutare se le garanzie offerte dal Fornitore siano sufficienti, prima di procedere con quest'ultimo alla stipula dell'accordo sul trattamento dei dati personali (c.d. Data Processing Agreement o DPA), contenente anche l'attribuzione della nomina quale Responsabile del trattamento. Alla luce anche del principio di *accountability*, la Fondazione, al cui interno opera l'OdM, deve infatti essere in grado di provare di aver tenuto in debita considerazione ogni elemento previsto dal GDPR, mentre il Fornitore quale Responsabile deve sempre essere in grado di dimostrare di poter garantire l'implementazione di

misure tecniche ed organizzative adeguate ad adempiere agli obblighi stabiliti dal GDPR. A seguito della verifica dei requisiti, una volta individuato il Responsabile idoneo, è necessario redigere un Accordo contenente le istruzioni sulle attività di trattamento da sottoscrivere con il Responsabile.

6.3. Valutazione dei requisiti richiesti dal GDPR

Una volta definito il ruolo del Fornitore eventualmente coinvolto nell'operazione di trattamento ed appurato che lo stesso agirà quale Responsabile, occorre che l'Organismo verifichi – e sia quindi in grado di dimostrare in un secondo momento – la sussistenza delle garanzie indicate dall'art. 28, comma 1, del GDPR, al fine di definire il DPA da stipularsi tra la Fondazione su proposta dell'OdM e il Fornitore quale Responsabile del trattamento).

Nella scelta del Responsabile per una data operazione di trattamento rilevano, come sopra anticipato, diversi fattori. Tra questi, dovrebbero essere presi in considerazione dall' OdM, al fine di valutare la sufficienza delle garanzie da parte del Responsabile:

1. le **conoscenze specialistiche**, ad esempio *l'expertise* tecnologica con riguardo alle misure di sicurezza implementate dal Fornitore a presidio dei dati da trattare per conto dell'Organismo, nonché, più in generale, di cui disporre in caso di verificazione di violazioni di dati personali (*data breach*) (ad es. accertata attraverso l'ottenimento della certificazione ISO 27001);

2. l'**affidabilità**, ad es. attraverso la conduzione da parte del Fornitore di *risk assessment* specifici per le operazioni di trattamento che si intende delegare, la nomina di un DPO anche in assenza dell'obbligo ai sensi di legge, o anche report finali di eventuali audit privacy, di prima o terza parte, effettuati sui processi e sui sistemi utilizzati dal Responsabile;

3. le **risorse** economiche (es. budget del DPO) e umane (es. l'organizzazione di *training* specifici o sessioni di formazione in materia di protezione dei dati personali a beneficio dei dipendenti) a disposizione per lo svolgimento delle operazioni di trattamento;

4. la **reputazione** sul mercato, ivi inclusi eventuali procedimenti aperti innanzi al Garante o all'autorità giudiziaria riguardanti possibili illeciti in materia di protezione dei dati;

5. l'eventuale **aderenza ad un codice di condotta** (diverso da quello per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale) ai sensi dell'articolo 40 del GDPR o a un **meccanismo di certificazione** a norma dell'art. 42 del Regolamento.

Inoltre, l'Organismo è chiamato a valutare se il Fornitore **consente di esercitare un sufficiente grado di controllo**, tenuto conto della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché dei possibili rischi per gli Interessati.

7. Attività di selezione dei Fornitori, di verifica dei requisiti e di stipula del Contratto

L'OdM è pertanto tenuto a:

1) in una prima fase, selezionare in coordinamento con la Fondazione i Fornitori a cui possono essere eventualmente delegate le relative attività di controllo e monitoraggio e verificarne il possesso dei requisiti richiesti dal Regolamento interno e dal GDPR, attraverso la richiesta e valutazione delle informazioni e documentazioni pertinenti, nonché apposite dichiarazioni e/o *checklist* da compilarsi predisposta a cura dell'OdM medesimo;
2) in una seconda fase, proporre alla Fondazione di procedere alla stipula del Contratto di servizi con il Fornitore prescelto e del connesso DPA ai sensi dell'art. 28 del GDPR, definendo in coordinamento con la Fondazione gli specifici obblighi e garanzie che il Fornitore dovrà assumere per garantire la massima riservatezza riguardo alle notizie, informazioni e dati di cui verrà a conoscenza nel corso dell'esecuzione dell'incarico affidatogli da parte dell'Organismo e per assicurare il rispetto delle istruzioni impartite relativamente alle attività ed operazioni da svolgere a tale fine;
3) successivamente, nel corso del rapporto con il Fornitore e fino alla sua cessazione, verificare il mantenimento dei suddetti requisiti e la corretta attuazione degli obblighi ed implementazione delle garanzie sufficienti per tutta la durata delle attività delegate al Fornitore, anche mediante checklist o relazioni periodiche (con cadenza almeno semestrale o annuale, a seconda della durata del Contratto).

8. Vigenza e modifiche alla presente Procedura

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

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

Questa Procedura potrà essere modificata, integrata o integralmente sostituita in ogni momento, previa approvazione da parte dell'Organismo, per garantire i necessari adeguamenti a nuove norme di legge e/o a provvedimenti dell'Autorità, oltre che alle migliori pratiche di settore.

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