ORGANISMO DI MONITORAGGIO

CODICE DI CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITÀ E PUNTUALITÀ NEI PAGAMENTI

POLICY SULL'ESECUZIONE DI ATTIVITÀ DI CONTROLLO E VERIFICA NEI CONFRONTI DEGLI ADERENTI

Premessa

L'Autorità Garante per la protezione dei dati personali (di seguito, il "**Garante Privacy**") nel 2019 ha approvato il *Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti*, ai sensi dell'art. 20 del d.lgs. 10 agosto 2018, n. 101, con le indicazioni contenute nel relativo provvedimento n. 163 del 12 settembre 2019; di seguito indicato anche come "**Codice di condotta**".

L'articolo 15 del citato Codice di condotta disciplina le "Verifiche sul rispetto del Codice di condotta ed organismo di monitoraggio", stabilendo che: "*Fatti salvi i compiti e i poteri del Garante di cui agli articoli da 56 a 58 del Regolamento, il rispetto del presente Codice di condotta per quanto attiene esclusivamente alle operazioni di trattamento di dati personali poste in essere dai gestori aderenti al presente Codice di condotta è garantito da un apposito organismo di monitoraggio (di seguito, l'"OdM") costituito e accreditato ai sensi dell'articolo 41 del Regolamento, la cui composizione e il cui funzionamento sono disciplinati nell'Allegato 4 al presente Codice di condotta*."

L'Allegato 4 del sopra menzionato Codice di condotta, all'art. 4, prevede che "*Ai fini del controllo del rispetto del presente Codice di condotta da parte di tutti i Gestori Aderenti, l'OdM potrà in ogni momento svolgere - anche delegandole a soggetti terzi nei limiti sopra indicati - tutte le verifiche ritenute opportune, ivi incluse ispezioni, sia in remoto che presso la sede dei Gestori Aderenti, tenuti a prestare la massima collaborazione ai fini del proficuo svolgimento di tali attività*"

Il presente documento fa riferimento oltre che al Regolamento (UE) 2016/679 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**"); al d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito il "**Codice**") come novellato dal d.lgs 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679"; al Codice di Condotta; al Regolamento interno, e, inter alia, alle fonti indicate nel Provvedimento del Garante per la protezione dei dati personali del 12 settembre 2019 relativo al Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti.

1. **Finalità e struttura della Policy**

La presente policy (di seguito, la "**Policy"**) stabilisce le regole e le procedure applicabili allo svolgimento di controlli ed ispezioni da parte dell'Organismo di monitoraggio (di seguito, l'"**OdM**" o l' "**Organismo**") costituito, ai sensi dell'articolo 41 del Regolamento al fine di garantire il rispetto del Codice di Condotta.

Questa Policy ha la finalità di:

- definire il metodo e l'iter di svolgimento delle attività di controllo e verifica previste dal Codice di Condotta nei confronti dei soggetti ad esso aderenti (i "**Gestori**");
- identificare le diverse fasi del procedimento e, per ciascuna di esse, le specifiche attività da espletarsi;
- dotarsi di uno strumento operativo in grado di favorire la corretta attuazione di quanto previsto dal Codice di Condotta e dal Regolamento interno.

2. Ambito di applicazione della Policy

La Policy si applica a qualsiasi attività di controllo svolta da parte dell'OdM ai sensi dell'art. 4 dell'Allegato 4 al Codice di condotta, a prescindere dalla forma di volta in volta prescelta (es. audit da remoto, ispezione in loco, richiesta di informazioni o chiarimenti, compilazione di questionari) 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 Gestori.

I soggetti destinatari (di seguito, i "**Destinatari**") di questa Policy sono:

- Componenti dell'Organismo, attuali e futuri, chiamati ad eseguire i controlli richiesti dal Codice di Condotta e dal Regolamento interno;
- i Gestori;
- le eventuali società terze agenti, ai fini dell'esecuzione dei controlli oggetto della presente Policy, per conto e su incarico specifico dell'OdM;
- il personale amministrativo eventualmente operante in favore dell'Organismo, qualora coinvolto in alcuna delle attività descritte nella presente Policy;

3. **Definizioni**

Salvo che sia diversamente previsto, ai fini della presente Policy si applicano le definizioni previste dall'art. 4 del Regolamento e le definizioni previste dall'art. 2 del Codice di condotta

4. **Casi 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 degli obblighi stabiliti dal Codice di Condotta, le attività di controllo avverranno in particolare nel caso in cui l'OdM lo reputi necessario sulla base della particolare frequenza e/o gravità dei reclami ricevuti o delle violazioni rilevate direttamente da parte dell'OdM stesso (di seguito, i "**Controlli occasionali**").

A prescindere da quanto sopra e quindi eventualmente in aggiunta ai Controlli occasionali scaturiti dalle circostanze descritte, l'OdM potrà svolgere annualmente verifiche di conformità al Codice di Condotta (di seguito, i "**Controlli routinar**i") nei confronti di un numero di Gestori, scelti per estrazione a sorte.

I criteri di selezione dei Gestori da sottoporre ai Controlli routinari sono definiti da parte dell'OdM, anche tenendo conto di decisioni, linee guida, piani ispettivi o provvedimenti di particolare rilievo eventualmente adottati dal Garante o dall'EDBP nei mesi precedenti, entro la fine di gennaio di ogni anno e possono essere integrati o rivisti nel corso dell'anno, previa apposita delibera dell'OdM stesso.

Qualora nel corso dello svolgimento di un Controllo routinario dovesse emergere l'esigenza di eseguire un Controllo occasionale sul medesimo Gestore, l'Organismo potrà decidere, a propria esclusiva discrezione ed eventualmente sentito il Gestore coinvolto, se sospendere o meno le attività di Controllo routinario per l'intera o parte della durata del Controllo occasionale.

5. **Tipologia di controlli eseguibili**

In conformità a quanto stabilito dal Codice di Condotta, l'Organismo può assolvere ai propri compiti di monitoraggio eseguendo tutte le verifiche ritenute opportune per accertare il puntuale rispetto, da parte del Gestore coinvolto, di tutte o solo di specifiche prescrizioni del Codice di Condotta.

Tali verifiche possono essere svolte, anche in ragione dei profili che l'Organismo intende specificamente appurare, mediante gli strumenti di controllo che quest'ultimo considera più idonei al raggiungimento degli obiettivi di volta in volta identificati. L'OdM può quindi esercitare tutti i poteri ispettivi necessari ad assicurare una puntuale ed efficiente vigilanza sull'osservanza del Codice di Condotta, tra cui a titolo esemplificativo:

- svolgere audit ed effettuare tutte le verifiche e le ispezioni ritenute opportune ai fini del corretto espletamento dei propri compiti, sia direttamente nei locali aziendali del Gestore che da remoto;
- avere libero accesso presso tutte le funzioni, gli archivi, i documenti, le infrastrutture e gli impianti del Gestore, senza alcun consenso preventivo o necessità di autorizzazione, al fine di ottenere ogni informazione, dato o evidenza documentale ritenuta necessaria;
- disporre, ove occorra, l'audizione di dipendenti, amministratori e dirigenti del Gestore, al fine di raccogliere informazioni o chiarimenti utili, concordando preventivamente gli impegni, sempre che non vi ostino ragioni d'urgenza;
- inviare richieste di informazione e di chiarimento e chiedere la compilazione di appositi questionari.

Fermo quanto sopra, le attività di controllo vengono di norma eseguite da parte dell'OdM da remoto, anche mediante sottoposizione al Gestore, di una checklist contenente almeno gli elementi di cui all'Allegato 1 della presente Policy e successivo invio, da parte del Gestore, di tutta la documentazione richiesta o, in aggiunta, comunque ritenuta utile a dimostrare, in ottica di *accountability*, la piena conformità al Codice di Condotta dei trattamenti svolti nell'ambito della fornitura di servizi di informazione creditizia. 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 Gestori, o dei loro responsabili del trattamento, al verificarsi delle circostanze che richiedono l'esecuzione di Controlli occasionali ai sensi del precedente paragrafo, o in caso di gravi mancanze o acclarate criticità emerse dalla checklist o dalla successiva analisi documentale.

6. Modalità e fasi di esecuzione dei controlli

In conformità a quanto previsto dal Codice di Condotta e nel rispetto dei requisiti stabiliti dal Regolamento interno, l'OdM può affidare a Società terze o consulenti (l'"**Auditor Esterno**") l'esecuzione di qualsiasi genere di attività di controllo e verifica, ad eccezione di quelle che presuppongono o determinano l'esercizio di poteri decisionali. Gli obblighi di cooperazione applicabili al Gestore, descritti in questa Policy, restano ovviamente immutati in tutte le ipotesi di controlli svolti da un Auditor Esterno su incarico e per conto dell'OdM.

I Controlli routinari richiedono un preavviso nei confronti del Gestore non superiore a una settimana lavorativa (5 giorni) dall'invio della comunicazione di avvio da parte dell'OdM o dell'Auditor Esterno. I Controlli occasionali potranno essere effettuati senza preavviso, salvo il caso in cui presuppongano un'ispezione in loco, per la quale l'OdM o l'Auditor Esterno daranno un preavviso di non oltre 48 ore.

I Gestori sono tenuti a prestare la massima collaborazione nei confronti dell'OdM, o dei soggetti da esso appositamente delegati, ai fini del proficuo svolgimento di tutte le attività di controllo di cui al precedente paragrafo. L'eventuale mancato adempimento di tale obbligo deve essere valutato da parte dell'OdM, insieme ad ogni altro elemento utile, in sede di decisione finale, all'esito delle attività di controllo, sul livello di conformità del Gestore al Codice di Condotta e alla normativa in materia di protezione dei dati personali.

Tutte le attività di monitoraggio e controllo svolte da parte dell'OdM ai sensi del Codice di Condotta ed in conformità alla presente Policy devono essere documentate in apposito verbale, da inviarsi al Gestore coinvolto entro 10 (dieci) giorni dalla chiusura delle relative operazioni. Gli addebiti eventualmente mossi nei confronti del Gestore devono essere motivati e circostanziati in una nota di accompagnamento al verbale, così che quest'ultimo possa, nei 15 (quindici) giorni lavorativi successivi, fornire chiarimenti a riguardo e presentare le proprie note di replica.

Qualora l'OdM, sulla base degli elementi acquisiti, ritenga di essere già in condizione di valutare compiutamente la questione, adotterà la propria decisione entro i 60 (sessanta) giorni lavorativi successivi. In caso contrario, l'OdM potrà richiedere al Gestore ulteriori 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.

Nel caso in cui venga disposta un'audizione, di cui deve essere redatto un sintetico verbale da inviare al Gestore entro i 5 (cinque) giorni successivi, la stessa avrà luogo presso la sede dell'OdM e nella data fissata

da quest'ultimo. In sede di audizione il Gestore potrà farsi assistere da un avvocato o da altro professionista munito di idoneo mandato.

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

7. Decisioni derivanti dai controlli

Al termine della procedura descritta al precedente paragrafo, svolte le necessarie discussioni riguardo ai risultati delle attività di verifica eseguite, l'OdM può stabilire di applicare al Gestore, motivando adeguatamente la decisione, tenuto conto della gravità della violazione riscontrata, una o più delle seguenti misure:

- un richiamo formale indirizzato esclusivamente al Gestore coinvolto;
- un richiamo da pubblicarsi in apposita sezione del sito web dell'Organismo;
- la sospensione temporanea dell'adesione del Gestore al Codice di Condotta;
- la revoca dell'adesione del Gestore al Codice di Condotta.

Le decisioni mediante cui vengano applicate misure di sospensione temporanea o di revoca dell'adesione del Gestore aderente al Codice di Condotta, devono essere trasmesse al Garante entro tre (3) giorni dalla loro adozione e, sempre ad opera del Presidente dell'OdM, essere pubblicate, anche in forma sintetica, previo oscuramento dei dati personali eventualmente presenti, in apposita sezione del sito web dell'Organismo, raggiungibile all'indirizzo www.odmsic.it.

8. Vigenza e modifiche alla presente Policy

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

Una copia di questo documento verrà messa a disposizione dei Destinatari tramite Posta Elettronica Certificata e sarà pubblicata sul sito web dell'OdM.

La presente Policy potrà essere modificata, integrata o integralmente sostituita in ogni momento, previa approvazione da parte della maggioranza dei componenti l'OdM, per garantire i necessari adeguamenti a nuove norme di legge e/o a provvedimenti del Garante per la protezione dei dati personali, 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. Nessuno dei Destinatari potrà giustificare la propria condotta adducendo la mancata conoscenza del presente documento.

ALLEGATO 1 – CHECKLIST BASE PER L'ESECUZIONE DI VERIFICHE PRESSO I GESTORI ADERENTI AL CODICE DI CONDOTTA

Modalità di raccolta, tipologia e registrazione dei dati (artt. 4; 5.3 Codice di condotta)

Modalità e richieste di verifica del gestore, anche a seguito dell'esercizio di un diritto da parte dell'interessato (art. 5.4 Codice di condotta)

Eventuali operazioni di cancellazione, integrazione o modificazione dei dati registrati in un SIC (art. 5.5 Codice di condotta)

Modalità di verifica dell'invio di solleciti o di altre comunicazioni con cui viene inviato all'interessato un preavviso circa l'imminente registrazione dei dati in uno o più SIC. (art. 5.6 Codice di condotta)

Informativa fornita agli interessati (art. 6 Codice di condotta)

Tempi di conservazione dei dati (art. 7 e Allegato 2 Codice di condotta)

Utilizzazione dei dati (art. 8 Codice di condotta)

Registro accesso ed esercizio diritti (art. 9 Codice di condotta)

Registro reclami/contestazioni (art. 9.6 Codice di condotta)

Trattamenti o processi decisionali automatizzati di scoring (art. 10 Codice di condotta)

Trattamento di dati provenienti da fonti pubbliche e/o da altre fonti (art. 11 Codice di condotta)

Misure di sicurezza dei dati (art. 12 Codice di condotta)

Notifica di una violazione dei dati personali (art. 13 Codice di condotta)

Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali (art. 14 codice di condotta)

Registri delle attività di trattamento (art. 30 RGPD)

Valutazione d'impatto sulla protezione dei dati (art. 35 RGPD)

Nomina Responsabile della Protezione dei Dati (art. 37 RGPD)