IN VIGORE IL CODICE DI CONDOTTA SULLO SVILUPPO E PRODUZIONE DI SOFTWARE GESTIONALE

29 novembre 2024

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Jessica Giussani
Associate

Giovanni Lombardi
Associate

Con la pubblicazione sulla Gazzetta Ufficiale n. 278 del 27 novembre 2024 della delibera del Garante per la protezione dei dati personali del 17 ottobre 2024, è stato definitivamente approvato il "Codice di Condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale" (il "Codice"). Tale provvedimento rappresenta un significativo passo avanti nell'implementazione di standard elevati di compliance nel settore dell'innovazione digitale.

Il Codice si inserisce nel quadro normativo delineato dall'art. 40 del Regolamento (UE) 2016/679 ("GDPR"), che promuove l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione della normativa privacy, tenendo conto delle specificità dei vari settori di trattamento e delle esigenze peculiari delle micro, piccole e medie imprese.

AMBITO DI APPLICAZIONE E FINALITÀ

Il perimetro applicativo del Codice comprende le imprese che si occupano della progettazione, dello sviluppo, della produzione e dell'assistenza di software gestionali, includendo altresì le attività di manutenzione e aggiornamento. La *ratio* sottesa a tale regolamentazione risponde all'esigenza, sempre più avvertita nel settore, di uniformare le prassi di trattamento dei dati personali, ponendo particolare enfasi sui principi di *privacy by design* e *privacy by default*: l'obiettivo primario è quello di garantire che i prodotti e i servizi sviluppati rispettino standard elevati di protezione dei dati sin dalla fase di progettazione, supportando efficacemente i titolari dei trattamenti nel processo di conformità al GDPR.

NOVITÀ PRINCIPALI

Tra gli aspetti maggiormente qualificanti del Codice, meritano particolare attenzione:

- l'implementazione dei principi di *privacy by design* e *by default*: viene sancito l'obbligo per le Software House ("**SWH**") di integrare, sin dalla fase di

progettazione, misure tecniche e organizzative adeguate per garantire la conformità normativa, secondo un approccio proattivo alla protezione dei dati;

- la definizione puntuale del ruolo delle SWH: viene cristallizzata la posizione delle *software house* quali responsabili o sub-responsabili del trattamento, con particolare riferimento alle attività di manutenzione e assistenza dei sistemi, sia in ambiente *on-premise* che *cloud*;
- la standardizzazione dei rapporti contrattuali: viene introdotto un modello di accordo *ex* art. 28 GDPR (nomi a responsabile del trattamento dei dati personali) per disciplinare organicamente i rapporti tra SWH e clienti in relazione ai trattamenti effettuati;
- l'istituzione di un Organismo di monitoraggio ("**OdM**"): è prevista la costituzione di un organismo accreditato dal Garante, con il compito di verificare l'osservanza del Codice, garantendo un controllo costante e qualificato sulla conformità delle prassi adottate.

IMPATTO OPERATIVO

Per le aziende produttrici di software gestionale, l'adesione al Codice si configura come uno strumento strategico di ***accountability***, contribuendo a rafforzare la fiducia dei clienti e degli utilizzatori finali. Gli strumenti operativi forniti - quali linee guida pratiche e modelli contrattuali standardizzati - rappresentano un supporto concreto particolarmente prezioso per le PMI, che spesso non dispongono internamente delle risorse tecniche necessarie per garantire una piena *compliance* al GDPR.

Dal punto di vista dei clienti utilizzatori, il Codice garantisce una maggiore trasparenza e uniformità nella gestione dei dati, permettendo di fare affidamento su partner tecnologici che implementano misure di sicurezza all'avanguardia secondo standard condivisi e verificati.

PROSPETTIVE FUTURE

L'entrata in vigore del Codice comporta una serie di adempimenti concreti per le *software house* che intendono aderirvi. In particolare:

sarà necessario effettuare una ***gap analysis*** preliminare rispetto ai requisiti del Codice, con particolare attenzione alle misure tecniche e organizzative richieste dagli allegati A e B;

dovranno essere rivisti i **modelli contrattuali** in uso, per allinearli allo schema di accordo ex art. 28 GDPR previsto dal Codice;

occorrerà predisporre o aggiornare le **procedure interne** per la gestione degli incidenti di sicurezza e delle richieste di esercizio dei diritti degli interessati;

andrà pianificata l'attività di formazione del personale sulle nuove procedure e sui requisiti del Codice.

È importante sottolineare che l'adesione al Codice è volontaria e non prevede termini perentori per la presentazione delle domande. Tuttavia, considerando che l'adesione rappresenterà sempre più un requisito qualificante nelle procedure di selezione dei fornitori di software gestionali, è consigliabile per le *software house* avviare tempestivamente il processo di valutazione dei requisiti e di eventuale adeguamento delle proprie procedure e strumenti, al fine di poter presentare la domanda di adesione non appena l'Organismo di monitoraggio sarà pienamente operativo.

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Jessica Giussani

Associate

Giovanni Lombardi

Associate