CONSERVAZIONE DOCUMENTALE E GDPR: DUE REGIMI SULLO STESSO DOCUMENTO

Perché il tempo è il vero punto di rottura nella compliance documentale dei soggetti vigilati

15 giugno 2026

AUTORI

Aurora Agostini
Partner

La conservazione "a norma" del documento informatico e la disciplina di protezione dei dati personali non sono binari paralleli: sono due regimi distinti che insistono sullo stesso processo e devono coesistere. Il punto di tensione più frequente è il tempo. L'art. 5, par. 1, lett. e), GDPR impone limiti che si combinano — talvolta in modo contraddittorio — con i termini documentali settoriali del TUB, della disciplina antiriciclaggio, della MiFID II e del DORA. Per banche e intermediari, riconciliare i due regimi è una scelta di governance che si misura in sede ispettiva e contenziosa.

LA CONSERVAZIONE È "TRATTAMENTO"

Nella quasi totalità dei casi rilevanti per un soggetto vigilato, il documento informatico contiene dati personali. La definizione dell'art. 4, n. 1, GDPR è ampia e, alla luce del considerando 26, ricomprende anche l'identificabilità indiretta: un IBAN o un codice cliente univoco, pur senza il nome accanto, restano dati personali. Il contratto di conto, la lettera di trasparenza, l'estratto conto, la registrazione del contact center, la segnalazione antiriciclaggio, il modulo di adeguata verifica, il log degli accessi all'home banking sono, allo stesso tempo, atti giuridicamente rilevanti e raccolte strutturate di dati personali.

Ne discende un passaggio scritto nella norma: l'art. 4, n. 2, GDPR nomina espressamente la «conservazione» fra le operazioni di trattamento. Alla conservazione documentale si applicano quindi per intero i principi dell'art. 5 e gli obblighi che ne derivano — informativa (artt. 13-14), registro dei trattamenti (art. 30), valutazione d'impatto quando il rischio è elevato (art. 35), misure di sicurezza (art. 32), base giuridica (art. 6), diritti dell'interessato (artt. 15-22). Sul piano operativo, ciò impone che il manuale della conservazione (par. 4.5 delle Linee Guida AgID) e il registro dei trattamenti (art. 30) dialoghino: stessi tempi, stesse misure di sicurezza, stessa catena di sub-responsabili. Quando non coincidono, il soggetto vigilato si espone su due fronti, davanti all'autorità di vigilanza e davanti al Garante.

Che i due regimi non si assorbano è confermato da un caso ormai di scuola: con il provv. 13 aprile 2023, n. 128 (doc. web 9888438), il Garante ha sanzionato un istituto che, dopo aver revocato una carta di credito sulla base di una banca dati

esterna usata a fini antiriciclaggio, non aveva riscontrato l'istanza di accesso ex art. 15 GDPR né reso un'informativa adeguata. La base giuridica AML (art. 6, par. 1, lett. c) legittima la conservazione, ma non assorbe gli obblighi di trasparenza e accesso — principio confermato dalla Corte di Giustizia UE in C-579/21 (Pankki S, 22 giugno 2023).

LA RETENTION DEI DATI: L'ART. 5(1)(E) COME PARAMETRO DI CHIUSURA

I dati vanno «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità» (art. 5, par. 1, lett. e). La norma non vieta di conservare oltre un termine: vieta di conservare *in forma identificabile* più a lungo del necessario — distinzione che apre la porta all'anonimizzazione, ammessa a tempo indeterminato.

Per i soggetti vigilati le fonti settoriali fissano ciascuna un proprio termine documentale (art. 119 TUB; artt. 31-32 D.Lgs. 231/2007, da leggere col Regolamento UE 2024/1624; art. 2220 c.c.; MiFID II e Reg. delegato UE 2017/565; DORA, Reg. UE 2022/2554). Rispetto a questo reticolo, l'art. 5(1)(e) opera come parametro di chiusura: può correggere verso il basso i termini sproporzionati rispetto alla finalità, ma non li espande oltre lo stretto necessario. La presenza di un obbligo legale legittima il *conservare*, non rende automatico il *conservare per X anni*. Coerentemente, il termine deve risultare — e coincidere — in tre luoghi: informativa (artt. 13-14), registro (art. 30, par. 1, lett. f) e manuale della conservazione (par. 4.5 Linee Guida AgID). È dalla discrepanza fra questi documenti che parte qualunque verifica ispettiva.

Il Garante ha fissato due regole nette su come i tempi vanno determinati. Primo: l'informativa non può limitarsi a riprodurre il testo dell'art. 5(1)(e) — clausole come «per la durata del rapporto e per i termini di legge» non superano più un audit (provv. 28 luglio 2022, doc. web 9843603) e vanno sostituite con indicazioni concrete, per categoria di dato e finalità. Secondo: i tempi vanno determinati per finalità specifica, non applicando un'unica fascia a categorie eterogenee di dati ("criteri a blocchi"), come confermato in una serie coerente di provvedimenti su geolocalizzazione, log di ex collaboratori e metadati di posta (tra gli altri, doc. web 9263597/2020 e 9920814/2023). Il prolungamento resta possibile, ma va richiesto e motivato anche nel *quantum*: nel caso di riferimento (verifica preliminare 18 aprile 2018, n. 233, doc. web 8997404) il Garante ha ridotto da 15 a 10 anni la conservazione dei dati di marketing, imponendo alla scadenza la cancellazione o l'anonimizzazione «permanente ed irreversibile».

In sintesi, una retention policy difendibile mappa per categoria di dato (non per documento) sul registro ex art. 30; associa a ciascuna categoria base giuridica,

finalità e termine motivato; applica il termine più lungo al solo dato minimo necessario; definisce la modalità di cessazione (cancellazione, anonimizzazione irreversibile o archiviazione segregata ex art. 89); e rende dimostrabile la cancellazione tramite log e registri, automatizzandola dove possibile (Linee Guida EDPB 4/2019). Una conservazione non documentabile in ispezione è di per sé un'inadempienza

DIRITTO ALL'OBLIO E OBLIO CREDITIZIO NEI SIC

Per i soggetti vigilati il diritto all'oblio è quasi sempre un bilanciamento fra obbligo di conservare e diritto alla cancellazione. L'art. 17 GDPR elenca i presupposti della cancellazione (par. 1) ma anche le eccezioni rilevanti (par. 3), fra cui l'adempimento di un obbligo legale (lett. b) e la difesa di un diritto in giudizio (lett. e); quando la cancellazione non è possibile, resta la limitazione del trattamento ex art. 18, par. 1, lett. b). Sul *delisting*, la Corte di Giustizia UE ha definito il perimetro da Google Spain (C-131/12, 2014) fino a TU e RE c. Google (C-460/20, 2022), che ha posto in capo al richiedente l'onere di provare l'inesattezza del dato. Utile in chiave operativa è il modello degli archivi storici dei quotidiani (Garante, doc. web 9577346/2021): l'oblio può realizzarsi per *segregazione* dell'archivio (deindicizzazione, accesso limitato) anziché per cancellazione — approccio ex art. 89 replicabile dalle banche per i dataset di clientela non più attiva.

Il caso più ricorrente è l'oblio creditizio nei sistemi di informazioni creditizie. La materia è governata dal Codice di condotta SIC (provv. Garante 12 settembre 2019, n. 163, doc. web 9141501): i tempi massimi (art. 6) decorrono dalla cessazione del comportamento e sono articolati per gravità — fino a sessanta mesi per le morosità non sanate — oltre i quali la segnalazione è illecita. Distinto è il regime della Centrale dei Rischi di Banca d'Italia (Circolare n. 139/1991), fondato sulla persistenza del rischio anziché su termini fissi: di fronte a una doglianza, la prima verifica è dunque la qualificazione del sistema. La Cassazione, con orientamento favorevole al debitore "riabilitato" (tra le altre, n. 33013/2018 e n. 16358/2020), ammette la cancellazione anche prima della scadenza dei tetti in presenza di circostanze qualificanti.

LE CONSEGUENZE OPERATIVE

Il messaggio operativo è che la conformità documentale non si esaurisce nella correttezza del processo di conservazione "a norma", né nell'adempimento isolato degli obblighi GDPR: si gioca nel punto di contatto fra i due regimi. Allineare manuale e registro, determinare i tempi per finalità concreta, progettare

cancellazione e anonimizzazione come processi automatizzati e dimostrabili, pre-cablare la matrice di notifica degli incidenti: è questo che distingue una compliance intesa come governance da una ridotta ad adempimento documentale — e una posizione che regge in ispezione e in giudizio da una che si sgretola al primo audit.

TEAM

Aurora Agostini

Partner

Giulietta Minucci

Partner

Marco Grechi

Senior Associate

Giovanni Lombardi

Associate

Alessandro Carlini

Associate

Francesca Costarelli

Associate

Alessia Spada

Associate