BANCA D'ITALIA
EUROSISTEMA

Documento per la consultazione

Disposizioni di attuazione dell'articolo 53, comma 2-*ter*, del decreto legislativo 1° settembre 1993, n. 385.

Il documento contiene uno schema di disposizioni attuative dell'art. 53, comma 2-*ter*, del Testo unico bancario, in materia di conservazione dei dati personali detenuti dai sistemi di informazione creditizia per finalità di sviluppo dei sistemi di rating.

Eventuali osservazioni, commenti e proposte possono essere trasmessi, entro 60 giorni dalla pubblicazione del presente documento, a:
Banca d'Italia, Servizio Normativa e Politiche di Vigilanza, Divisione Normativa prudenziale, via Milano 53 – 00184 ROMA, oppure all'indirizzo di posta elettronica *npv.normativa_prudenziale@bancaditalia.it*.

Maggio 2010

BANCA D'ITALIA
EUROSISTEMA

RELAZIONE ILLUSTRATIVA

L'art. 53, comma 2-*ter*, del d.lgs. 1° settembre 1993, n. 385 (Testo unico bancario - TUB) ([1]) dispone che "*Le società o enti esterni che, anche gestendo sistemi informativi creditizi, rilasciano alle banche valutazioni del rischio di credito o sviluppano modelli statistici per l'utilizzo ai fini di cui al comma 1, lettera a), conservano, per tale esclusiva finalità, anche in deroga alle altre vigenti disposizioni normative, i dati personali detenuti legittimamente per un periodo di tempo storico di osservazione che sia congruo rispetto a quanto richiesto dalle disposizioni emanate ai sensi del comma 2-bis. Le modalità di attuazione e i criteri che assicurano la non identificabilità sono individuati su conforme parere del Garante per la protezione dei dati personali*".

L'accluso schema normativo, diretto a dare attuazione alla previsione di legge, tiene conto di osservazioni e suggerimenti formulati dal Garante per la protezione dei dati personali nel corso di una fase di confronto preliminare. L'emanazione delle disposizioni, una volta concluso il processo di consultazione, resta condizionata al previo parere conforme dell'Autorità Garante, in conformità di quanto previsto dalla citata norma del TUB.

° ° °

Lo schema del provvedimento – che si compone di un articolato e di un allegato tecnico – reca anzitutto le **definizioni** dei termini tecnici ricorrenti nel provvedimento (**art. 1**), che riproducono analoghe previsioni contenute nelle fonti normative richiamate nel preambolo del provvedimento stesso (Codice in materia di protezione dei dati personali e Codice di deontologia, Testo unico bancario, disposizioni di vigilanza prudenziale per le banche).

Sono quindi precisate **le finalità e i limiti** in relazione ai quali il trattamento dei dati da parte dei gestori dei sistemi di informazione creditizia (SIC) sarebbe consentito oltre i termini previsti in via generale dalla normativa sulla *privacy* ([2]). In particolare, le finalità sono esclusivamente quelle di sviluppo, da parte delle banche e dei gestori dei SIC, di modelli statistici da utilizzare nell'ambito di sistemi di rating, nel rispetto della condizione di non identificabilità (**art. 2**);

---

(1) La previsione è stata introdotta dal decreto-legge 27 dicembre 2006, n. 297, convertito, con modificazioni, dalla legge 23 febbraio 2007, n. 15, con cui sono state apportate modifiche ai Testi unici bancario e della finanza per recepire nell'ordinamento italiano le novità introdotte dalle direttive comunitarie 2006/48/CE e 2006/49/CE, relative all'accesso all'attività bancaria e all'adeguatezza patrimoniale delle banche e delle imprese di investimento.

(2) Questa consente di conservare i dati gestiti dai SIC per un periodo variabile a seconda della tipologia di informazioni e comunque mai superiore a 3 anni (cfr. Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti, adottato con Provvedimento del Garante per la protezione dei dati personali n. 8 del 16 novembre 2004).

Sono poi stabiliti **criteri di conservazione, accesso e utilizzo dei dati**, tali da rendere i dati non identificabili né accessibili da parte delle banche e dei SIC, salvo eccezioni tassativamente indicate e nel rispetto di specifiche cautele tecnico-organizzative (**artt. 3-4 e allegato tecnico**). In tale ambito:

i) sono individuati i casi di accesso ai dati da parte delle banche, strettamente correlati alle finalità di sviluppo dei modelli, e da parte dei gestori dei SIC, nei casi eccezionali in cui ciò sia necessario per assicurare la qualità dei dati;

ii) sono stabiliti termini massimi di conservazione dei dati da parte dei SIC e delle banche, che tengono conto dell'esigenza di rispettare i requisiti di profondità storica stabiliti dalla normativa prudenziale per le banche e di minimizzare i rischi di utilizzo per finalità diverse da quelle consentite;

iii) vengono disciplinate le modalità tecniche di conservazione e accesso, in modo da prevenire la possibilità di utilizzo dei dati per finalità diverse ed assicurare la non identificabilità dei dati stessi.

In particolare, si prescrive che i SIC debbano rendere anonimi i dati dei soggetti interessati mediante l'applicazione di meccanismi di crittografia a chiave pubblica con l'intervento di soggetti accreditati; i dati così anonimizzati sono conservati presso una struttura organizzativa separata da quella che gestisce gli archivi correnti del SIC; la chiave privata (che consente di compiere l'inversa operazione di deanonimizzazione, nei casi eccezionali in cui questa sia necessaria per finalità coerenti con lo sviluppo dei sistemi di rating) è custodita presso un terzo di fiducia e non è in alcun momento messa a disposizione dei gestori.

Il trattamento da parte dei SIC dei dati anonimizzati è circondato da presìdi tecnici comportanti, tra l'altro, la registrazione nominativa degli accessi agli archivi, l'applicazione di procedure volte a impedire flussi di dati verso archivi diversi, la separazione delle abilitazioni di accesso del personale autorizzato.

L'accesso delle banche ai dati conservati nell'archivio separato del SIC è consentito soltanto previa applicazione di una stessa chiave di crittografia pubblica sia sui dati trasmessi dal SIC sia su quelli eventualmente estratti dagli archivi interni della banca; i dati così acquisiti dalla banca devono essere conservati in archivi separati rispetto a quelli di produzione, con il ricorso a procedure interne di segregazione.

Infine, per assicurare l'effettiva applicazione degli obblighi imposti dalle nuove disposizioni i SIC e le banche dovranno predisporre apposite **procedure interne**, formalizzate e approvate dai competenti organi di vertice, il cui rispetto è verificato dalle funzioni di revisione interna e *compliance* (**art. 5**).

Schema delle disposizioni di attuazione dell'articolo 53, comma 2-*ter*, del decreto legislativo 1° settembre 1993, n. 385.

La BANCA D'ITALIA

VISTO il decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni, recante il testo unico delle leggi in materia bancaria e creditizia (Testo unico bancario); viste, in particolare, le seguenti disposizioni:

— l'articolo 53, comma 1, lettera *a)*, il quale prevede che la Banca d'Italia, in conformità delle deliberazioni del CICR, emana disposizioni di carattere generarle aventi a oggetto l'adeguatezza patrimoniale, rispettivamente, delle banche e dei gruppi bancari;

— l'articolo 53, comma 2-*bis*, lettera *b)*, il quale stabilisce che le disposizioni emanate ai sensi del comma 1, lettera *a)*, del medesimo articolo prevedono che le banche possano utilizzare sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, previa autorizzazione della Banca d'Italia;

— l'articolo 53, comma 2-*ter*, il quale prevede che le società o gli enti esterni che, anche gestendo sistemi informativi creditizi, rilasciano alle banche valutazioni del rischio di credito o sviluppano modelli statistici per l'utilizzo ai fini di cui al comma 1, lettera *a)*, del medesimo articolo conservano, per tale esclusiva finalità, anche in deroga alle altre vigenti disposizioni normative, i dati personali detenuti legittimamente per un periodo storico di osservazione che sia congruo rispetto a quanto richiesto dalle disposizioni emanate ai sensi del comma 2-*bis* dello stesso articolo. Le modalità di attuazione e i criteri che assicurano la non identificabilità sono individuati su conforme parere del Garante per la protezione dei dati personali;

VISTO il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante il Codice in materia di protezione dei dati personali;

VISTO il provvedimento del Garante per la protezione dei dati personali n. 8 del 16 novembre 2004, con il quale è stato adottato il Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (Codice di deontologia);

VISTA la Circolare della Banca d'Italia 27 dicembre 2006, n. 263 e successivi aggiornamenti (disposizioni di vigilanza prudenziale per le banche), con cui sono state recepite le direttive 2006/48/CE e 2006/49/CE del Parlamento europeo e del Consiglio del 14 giugno 2006 relative all'accesso all'attività degli enti creditizi ed al suo esercizio e all'adeguatezza patrimoniale delle imprese di investimento e degli enti creditizi;

CONSIDERATO che le banche e i gruppi bancari sono tenuti a predisporre i sistemi interni di determinazione dei requisiti patrimoniali in conformità delle disposizioni emanate dalla Banca d'Italia in attuazione delle richiamate direttive comunitarie;

RITENUTA l'esigenza che il trattamento dei dati da parte delle società ed enti esterni di cui all'articolo 53, comma 2-*ter*, del Testo unico bancario avvenga, nel rispetto delle esigenze di tutela della riservatezza dei dati, con modalità idonee a consentirne l'effettivo utilizzo da parte del sistema bancario ai fini della realizzazione di sistemi di determinazione dei requisiti patrimoniali;

ACQUISITO il conforme parere del Garante per la protezione dei dati personali in data…

ADOTTA

le seguenti disposizioni:

Articolo 1
(*Definizioni*)

1. Ai fini delle presenti disposizioni si definiscono:

— *sistema di informazioni creditizie (SIC)*: ogni banca di dati concernenti richieste/rapporti di credito, gestita in modo centralizzato da una persona giuridica, un ente, un'associazione o un altro organismo in ambito privato e consultabile solo dai soggetti che comunicano le informazioni in essa registrate e che partecipano al relativo sistema informativo. Il sistema può contenere, in particolare:

   1. informazioni creditizie di tipo negativo, che riguardano soltanto rapporti di credito per i quali si sono verificati inadempimenti;
   2. informazioni creditizie di tipo positivo e negativo, che attengono a richieste/rapporti di credito a prescindere dalla sussistenza di inadempimenti registrati nel sistema al momento del loro verificarsi;

— *gestore*: il soggetto privato titolare del trattamento dei dati personali registrati in un sistema di informazioni creditizie e che gestisce tale sistema stabilendone le modalità di funzionamento e di utilizzazione;

— *banca*: l'impresa autorizzata all'esercizio dell'attività bancaria;

— *sistema di rating*: l'insieme strutturato e documentato delle metodologie, dei processi organizzativi e di controllo, delle modalità di organizzazione delle basi dati che consenta la raccolta e l'elaborazione delle informazioni rilevanti per la formulazione di valutazioni sintetiche della rischiosità di una controparte e delle singole operazioni creditizie, così come definito dal Titolo II, Capitolo 1, Parte Seconda, Sezione I, paragrafo 3.1, delle disposizioni di vigilanza prudenziale per le banche;

— *trattamento*: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

— *dato personale*: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

— *dati identificativi*: i dati personali che permettono l'identificazione diretta dell'interessato.

Articolo 2
(*Finalità e ambito di applicazione*)

1. Il presente provvedimento disciplina il trattamento dei dati personali detenuti dai gestori dei SIC all'esclusivo fine dello sviluppo, in proprio o da parte delle banche, di modelli statistici da utilizzare nell'ambito di sistemi di rating con modalità e criteri idonei ad assicurare la non identificabilità degli interessati a cui si riferiscono i dati personali.

2. Ai fini e nei limiti di cui al comma 1, i gestori dei SIC possono trattare i dati legittimamente detenuti per il tempo previsto dalle disposizioni di vigilanza prudenziale

per le banche, anche in deroga alle previsioni del Codice di deontologia.

3. Le presenti disposizioni non riguardano la conservazione ad uso interno, da parte delle banche, della documentazione contrattuale o contabile contenente i dati personali relativi a richieste e rapporti di credito con la clientela.

Articolo 3
(*Conservazione e trattamento dei dati*)

1. Decorsi i termini di conservazione dei dati previsti dall'articolo 6 del Codice di deontologia, i gestori dei SIC possono trattare i dati personali per le finalità di cui all'art. 2, comma 1, previa la loro elaborazione secondo le procedure informatiche e gli accorgimenti tecnici e organizzativi di cui all'allegato.

2. I gestori dei SIC definiscono, con apposita delibera dell'organo amministrativo, il termine massimo, comunque non superiore a 20 anni, per la detenzione dei dati di cui al comma 1, tenendo conto dell'esigenza di assicurare una profondità delle serie storiche coerente con le finalità di sviluppo dei sistemi di rating e di minimizzare i rischi di utilizzo abusivo.

Articolo 4
(*Accesso ai dati*)

1. Le banche hanno accesso ai dati personali elaborati nei modi indicati all'articolo 3 esclusivamente per le finalità di cui all'articolo 53, comma 1, lettera *a)*, e comma 2-*bis*, e all'articolo 67, comma 1, lettera *a)*, e comma 2-*bis*, del Testo unico bancario, nel rispetto delle modalità specificate nell'allegato.

2. I gestori dei SIC hanno accesso ai medesimi dati al fine di mantenere un livello di qualità adeguato in relazione alle finalità di cui all'articolo 2, comma 1, esclusivamente ove necessario a seguito di rettifiche dei dati e per l'aggiornamento dei profili storici a seguito di istanze degli interessati.

3. L'accesso di cui al comma precedente è consentito esclusivamente con una procedura formalizzata nel rispetto delle modalità specificate nell'allegato. L'organismo di cui all'articolo 13, comma 7, del Codice di deontologia effettua verifiche periodiche sul rispetto delle modalità e condizioni di accesso dei SIC e trasmette il relativo verbale entro 30 giorni al Garante per la protezione dei dati personali.

4. Salvo quanto previsto dai commi precedenti, i gestori dei SIC possono accedere ai dati in forma anonima per finalità di sviluppo e aggiornamento dei modelli statistici, in conformità di quanto previsto dall'articolo 6, comma 8, del Codice di deontologia.

Articolo. 5
(*Controlli*)

1. Le banche e le società capogruppo predispongono una procedura formalizzata per l'accesso ai dati trattati dai SIC ai sensi delle presenti disposizioni. La procedura è approvata dall'organo con funzione di gestione, con il parere dell'organo di controllo.

2. Le funzioni di conformità alle norme e di revisione interna della banca o del gruppo bancario verificano periodicamente il rispetto della procedura e, con cadenza almeno annuale, riferiscono all'organo di controllo circa i risultati delle verifiche.

Allegato tecnico-organizzativo

Conservazione dei dati da parte dei SIC (art. 3)

Decorsi i termini di conservazione previsti dall'articolo 6 del Codice di deontologia, i gestori dei SIC, in qualità di titolari del trattamento, rendono anonimi i dati identificativi mediante la loro sostituzione con pseudonimi che non consentano l'identificazione diretta o indiretta dell'interessato cui si riferiscono. A tal fine, si fa ricorso a metodi di cifratura a chiave pubblica.

Il gestore del SIC chiede ad un certificatore accreditato nell'elenco gestito dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione la produzione di una coppia di chiavi pubblica e privata, con il rilascio di un certificato di firma digitale idoneo alla cifratura di documenti.

La chiave pubblica viene conservata dal gestore del SIC ed utilizzata per le opportune lavorazioni all'interno dello stesso SIC (anonimizzazione dei dati riferiti a periodi non coperti dal Codice di deontologia, cifratura dei dati ricevuti dalle banche ex art.4 comma 1, cfr. par. 2).

Il supporto contenente la corrispondente chiave privata viene depositato presso un soggetto terzo di fiducia e non deve trovarsi mai nella disponibilità del gestore del SIC.

La gestione e la conservazione separata dei dati personali resi anonimi rispetto agli altri dati di pertinenza del SIC è affidata ad un'apposita struttura organizzativa, autonoma e distinta da quella che gestisce i SIC, disciplinata da idonee procedure formalizzate.

Il processo di conservazione dei dati garantisce:

- la completezza, l'immodificabilità e l'autenticità delle registrazioni nominative degli accessi agli archivi anonimizzati detenuti per le finalità di cui all'art. 2 comma 1 nonché delle operazioni compiute dagli incaricati;
- la impossibilità di qualsiasi flusso di dati dagli archivi anonimizzati verso gli archivi in chiaro gestiti dal SIC per le finalità riconosciute dal Codice deontologico;
- l'assenza di utenti con un doppio accesso agli archivi in chiaro e anonimizzati.

Accesso ai dati da parte delle banche (art. 4 comma 1)

Le banche aderenti al SIC possono chiedere, per le finalità di cui all'art. 4 comma 1, la intera serie storica dei dati riferiti ad un campione di soggetti, di numero non esiguo, identificati sulla base delle proprie esigenze statistiche e di sviluppo dei modelli interni.

A tal fine, la banca comunica al SIC un elenco di codici identificativi dei clienti, crittografati utilizzando la chiave pubblica del SIC e secondo un tracciato record concordato.

All'interno del SIC, la struttura autonoma che detiene i dati crittografati (cf. sopra) estrae dalla base dati anonimizzata le serie storiche individuali per il campione e per il periodo di tempo richiesto e li invia alla banca distinguendo i soggetti con un codice sequenziale, tale da garantire che ciascun record della serie storica sia univocamente riferito ad un unico cliente compreso nella lista inviata dalla banca.

Ove la banca, in conformità di quanto previsto dalle disposizioni di vigilanza prudenziale, debba associare dati interni a quanto ricevuto dal SIC, essa fa esplicita richiesta al gestore del SIC di ricevere i dati completi del codice identificativo crittografato con la chiave pubblica di cui al par. 1. La banca costituisce un archivio parallelo con le informazioni da associare ai dati provenienti dal SIC, in cui i dati identificativi sono resi anonimi con la stessa chiave pubblica adottata dal SIC. I dati personali contenuti nell'archivio parallelo sono conservati per un periodo congruo rispetto a quanto richiesto dalle disposizioni di vigilanza prudenziale, comunque non superiore a 20 anni.

Le procedure interne della banca garantiscono la segregazione dei dati in modo che non sia possibile identificare i clienti presenti nell'archivio parallelo.

Accesso ai dati da parte dei SIC (art. 4 comma 3)

Per consentire ai gestori dei SIC l'accesso ai dati *in chiaro* nei casi previsti dall'art. 4 comma 2, è necessario l'intervento del soggetto terzo depositario della chiave privata corrispondente a quella pubblica utilizzata dal gestore del SIC per l'attività di cui sopra.

Il soggetto terzo provvede a comunicare al SIC la chiave privata da utilizzarsi secondo quanto previsto da

un’apposita procedura formalizzata che disciplina le modalità dell’accesso (deanonimizzazione).

La procedura prevede anche l’immediata rianonimizzazione dei dati aggiornati con l’applicazione di una nuova chiave pubblica da gestirsi con modalità analoghe a quanto descritto in precedenza. La nuova chiave privata corrispondente alla chiave pubblica correntemente utilizzata dal SIC viene affidata in custodia al soggetto terzo di fiducia.