[vedi anche newsletter del 2 agosto 2013]

[doc. web n. 2563133]

Parere del Garante sullo schema di "Linee-guida per il Disaster Recovery delle pubbliche amministrazioni", emanate ai sensi dell'articolo 50-*bis*, comma 3, lett. b), del Codice dell'amministrazione digitale - 4 luglio 2013

Registro dei provvedimenti
n. 333 del 4 luglio 2013

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott. ssa Augusta Iannini, vice presidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti e del dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere dell'Agenzia per l'Italia digitale;

Visto l'articolo 50-*bis*, comma 3, lettera b), del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82);

Visto l'articolo 154, comma 1, lett. g), del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore la dott.ssa Augusta Iannini;

PREMESSO

L'Agenzia per l'Italia digitale ha richiesto il parere del Garante in ordine a uno schema di "Linee-guida per il *Disaster Recovery* delle pubbliche amministrazioni" emanate ai sensi dell'articolo 50-*bis*, comma 3, lett. b), del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni (*infra* CAD).

In base a tale disposizione normativa, infatti, le pubbliche amministrazioni definiscono il piano di *disaster recovery* (di seguito DR), che costituisce parte integrante del piano di continuità operativa e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. Al riguardo, l'Agenzia per l'Italia digitale, sentito il Garante, definisce, appunto, le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verificando annualmente il costante aggiornamento dei piani di DR delle amministrazioni interessate.

Una prima versione delle Linee guida era stata emanata nel novembre 2011, e sul relativo schema il Garante aveva espresso parere favorevole con condizioni e raccomandazioni (parere del 20 ottobre 2011).

RILEVATO

1. L'impianto generale delle Linee guida.
Lo schema di Linee-guida affronta il tema degli obiettivi e degli scenari della continuità operativa delle pp. aa. nel quadro normativo attuale, ed in particolare gli aspetti del DR (cap. 1), e delinea, al contempo, i ruoli e le responsabilità attribuite alle pp. aa. e all'Agenzia per l'Italia digitale nell'ambito della *Digital Agenda*, descrivendo altresì gli obblighi e gli adempimenti previsti nel Codice in materia di protezione dei dati personali (*infra* Codice) con riferimento alle misure di sicurezza (cap. 2).

Rilevano inoltre le infrastrutture e l'organizzazione della p. a. in materia di continuità operativa (cap. 3), la realizzazione della continuità operativa e delle soluzioni di DR (con riferimenti alle soluzioni *cloud*) (cap. 4), le modalità di redazione degli studi di fattibilità tecnica, dei piani di continuità operativa e dei piani di DR (cap. 5) e gli strumenti giuridici e operativi per l'acquisizione di un servizio di DR (che tratta anche le clausole da adottare per soluzioni *cloud* che implichino il trasferimento dei dati con rinvio alla normativa europea e ai provvedimenti del Garante) (cap. 6).

Il provvedimento tratta poi aspetti della continuità operativa e del DR nel contesto delle cc.dd. infrastrutture critiche, senza introdurre specificità di rilievo riguardo agli aspetti di protezione dei dati personali affrontati nei capitoli precedenti (cap. 7).

Infine, costituiscono parte del provvedimento anche cinque appendici, volte a proporre politiche di *back up* (appendice A), standard di

riferimento per l'attuazione della continuità operativa (appendice B), il modello di piano di continuità ICT (appendice C), specificazioni sugli strumenti giuridici ed operativi per l'acquisizione dei servizi di continuità operativa/*DR* (appendice D) e esempi di livelli di servizio (appendice E).

2. Definizioni.
Lo schema riproduce molte delle definizioni già contenute nel provvedimento in vigore.

In particolare, secondo il glossario, con il termine "disaster" si intende, ai fini del provvedimento in esame, "*l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione*", laddove la nozione di DR configura invece "*l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare indisponibilità prolungate*". Il DR comprende quindi le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture *hardware*, *software* e di servizi di comunicazione.

Si delineano, tra gli altri, i concetti di copia dei dati e delle applicazioni (*data mirroring*), di *database*, di dato, di dato delle pp. aa., di fruibilità di un dato, di allineamento dei dati, di *log*, di piano di continuità operativa ICT (PCO), di politiche di sicurezza, di *Recovery Point Objective* e di sistema pubblico di connettività.

Vi sono, poi, elementi di novità, come la definizione dell'Agenzia per l'Italia digitale, subentrata a *DigitPA*.

Infine, lo schema precisa che per *data center* si intende una struttura fisica insieme a tutti gli impianti e a sistemi di sicurezza fisica e logica presenti, progettato per gestire un numero elevato di apparecchiature e infrastrutture informatiche e i dati ivi contenuti, allo scopo di garantirne la sicurezza fisica e gestionale. Al riguardo, il Capitolo 3 sulle infrastrutture e l'organizzazione IT per la continuità operativa prevede, per la protezione degli stessi, una serie di misure di sicurezza, tra le quali rilevano il monitoraggio delle aree esterne ad opera di barriere infrarossi e/o sistemi di video analisi e sistemi di videosorveglianza con videoregistrazione, l'identificazione visiva personale a mezzo nastri porta *badge* di identificazione e la procedura di accesso al *data center*.

3. L'odierno schema di Linee guida alla luce del parere del Garante del 2011.
Da un'analisi dell'attuale schema di Linee guida in parallelo con quello precedente, emerge che sostanzialmente il nuovo testo accoglie le condizioni e le raccomandazioni adottate dal Garante nel parere del 20 ottobre 2011.

In particolare, rilevano i seguenti aspetti.

3.1. Politiche di *backup*.
Per quanto riguarda le "politiche di backup", nell'Appendice A (nella versione precedente § 4.5), si prevede che al fine di ottemperare a regole specificamente indicate e di semplificare i processi di gestione, le specifiche scelte organizzative e di processo devono essere rappresentate all'interno del Piano di continuità operativa (PCO) e, per la parte di propria competenza, nel Piano di DR, avendo cura di rendere allineati i dati nei sopra citati documenti.

Nella precedente versione (§ 4.5) il riferimento era ai soli documenti programmatici per la sicurezza e al riguardo il Garante, nel parere, aveva richiesto che, dal momento che non tutti i titolari del trattamento erano tenuti alla redazione del DPS (cfr. art. 34, comma 1-*bis* del Codice, all'epoca in vigore), la sede più idonea per documentare le scelte anche implementative in materia di procedure per il salvataggio periodico dei dati fosse proprio il Piano sulla continuità operativa e, in quell'ambito, il Piano per il DR, che devono invece essere obbligatoriamente redatti da tutte le pp. aa.. La nuova formulazione delle Linee guida si adegua alla condizione del Garante, anche se, per altro verso, dovrà essere espunto il riferimento al DPS, nel frattempo soppresso (v. avanti, par. 4).

3.2. Conservazione dei dati.
Per quanto riguarda il periodo di conservazione dei dati di *backup*, sempre nell'Appendice A (nella vecchia versione § 4.5.3), si stabilisce che i salvataggi devono avere un "periodo di ritenzione", passato il quale vengono eliminati; tale periodo deve essere commisurato alle finalità della conservazione dell'informazione (dei dati, delle applicazioni e dei processi) e deve essere precisamente indicato in tutti i documenti interessati (Piano di Continuità Operativa (PCO); Piano di DR (PDR)). Nella precedente versione del provvedimento, si prevedevano, invece, periodi di conservazione anche illimitati e il Garante aveva ritenuto tale previsione non conforme al principio di finalità nel trattamento di dati personali (cfr. art. 11, comma 1, lett. b) ed e), del Codice).

Analogamente, ancora nell'Appendice A ("Archiviazioni") si prevede che tutti o parte dei dati salvati siano oggetto di archiviazione su dispositivi che ne preservano l'integrità per periodi commisurati alle finalità di conservazione delle informazioni precisamente indicati nei documenti interessati (DPS, PCO, PDR), prevedendo le misure di conservazione relative al mantenimento dell'efficiente funzionalità del sistema informativo. Ai fini delle politiche di archiviazione storico documentale, le pp. aa. si dovranno attenere a quanto definito nell'ambito del "Manuale di Conservazione" che ne contiene le regole e i tempi. Nella versione precedente del provvedimento (§ 4.5.7), si prevedeva l'archiviazione periodica di tutti o parte dei dati su dispositivi che ne preservassero l'integrità per lunghi periodi e il Garante aveva rilevato nel parere che anche per tale conservazione fosse necessario individuare termini definiti, distinguendo le misure necessarie al mantenimento dell'efficiente funzionalità del sistema informativo e alla protezione dei dati in esso trattati dagli accorgimenti preordinati, invece, a realizzare forme di archiviazione storico-documentale. La nuova formulazione si adegua al parere.

3.3. Tecniche di cifratura.
Per quanto riguarda l'utilizzo di tecniche di cifratura, le Linee guida stabiliscono che tali tecniche non devono pregiudicare la disponibilità dei dati in caso di necessità, e che, pertanto, deve essere assicurata a tale scopo la compatibilità tecnologica dei supporti, dei formati di registrazione, degli strumenti crittografici e degli apparati di lettura dei dati per tutta la durata della conservazione del dato (Appendice A - "Ubicazioni"). Tali precisazioni e garanzie erano state espressamente richieste dal Garante nel parere.

3.4. Servizi *cloud*.
Un altro aspetto in ordine al quale sono state recepite le indicazioni rese dall'Autorità nel parere del 2011 riguarda l'utilizzo di servizi *cloud* per la realizzazione del PCO e di DR, che implichino il trasferimento di dati (par. 4.3.2.2 e 6.5; nella precedente versione § 5.3.2.3). Al

riguardo l'odierno schema dopo aver precisato che in relazione alla natura particolare dei servizi *cloud*, la p. a. deve considerare la possibile localizzazione della infrastruttura geograficamente distribuita, individua gli strumenti e le clausole da adottare per soluzioni *cloud* che implichino il trasferimento dei dati (con rinvio alla normativa comunitaria e ai provvedimenti del Garante).

In conformità ad una condizione prevista nel precedente parere, l'odierno schema di provvedimento prevede che il fornitore indichi "con apposita dichiarazione resa in sede contrattuale, l'esatta localizzazione, o le esatte localizzazioni dei dati gestiti".
Questo specifico aspetto è di estrema importanza.

Solo attraverso tale previsione, infatti, il titolare del trattamento è in condizione di valutare se questa particolare modalità di realizzazione del servizio rispetti effettivamente la normativa in materia di protezione dei dati personali e segnatamente l'articolo 45 del Codice, che vieta il trasferimento "anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea", qualora "l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato", a tal fine valutandosi anche "le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza". Inoltre, considerato che le legislazioni, anche in materia di protezione dei dati, possono essere molto diverse nei Paesi terzi e non garantire livelli di protezione adeguati, il nuovo § 6.5 prevede la necessità di agire contrattualmente, applicando delle clausole specifiche elaborate dalla Commissione Europea nei contratti di fornitura del servizio. Le predette clausole, effettive dal 15 maggio 2010, trasferiscono parte delle responsabilità sul trattamento dati a chi effettivamente tratta i dati. Considerato che l'attività di *outsourcing* può essere subappaltata anche più volte, nell'ambito del medesimo servizio, deve comunque essere garantita chiarezza su chi sia il responsabile per la sicurezza dei dati.

Sempre nel medesimo paragrafo, in conformità ad una raccomandazione prevista nel precedente parere che richiedeva di valutare l'opportunità di inserire un riferimento al documento del Garante "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*", si segnala l'importanza di consultare anche il predetto documento nonché la miniguida "Cloud Computing. – Proteggere i dati per non cadere dalle nuvole", pubblicata dal Garante nel maggio del 2012.

Con riferimento all'Appendice D ("Specificazioni sugli strumenti giuridici ed operativi per l'acquisizione dei servizi di CO/DR"), ed in particolare alle indicazioni per l'elaborazione delle clausole contrattuali per regolamentare i servizi e le soluzioni di CO/DR (D.2), nell'ambito del servizio di copia e allineamento dei dati (nella precedente versione § 6.3.1) si precisa, in conformità ad una raccomandazione prevista nel precedente parere del Garante, "l'importanza di osservare i provvedimenti fra cui il provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministrazione di sistema" del 27 novembre 2008".

3.5 Strumenti per l'autovalutazione.
All'interno del Capitolo 4 dedicato alle soluzioni di DR, si disciplinano, tra le altre cose, gli strumenti per l'autovalutazione cui è tenuta ogni amministrazione per analizzare le criticità. In particolare, la stima sulle criticità deve essere svolta secondo tre direttrici: la direttrice del servizio, la direttrice dell'organizzazione e la direttrice della tecnologia, nell'ambito delle quali s'individuano specifici indicatori ai fini della valutazione (cc. dd. criteri di stima). Con riferimento alla direttrice del servizio i criteri sono, tra gli altri, il tipo di dati trattati, la possibilità di recuperare la mancata acquisizione dei dati e la necessità di recuperare i dati non acquisiti. Per quanto riguarda, invece, la direttrice dell'organizzazione, rilevano fra le varie ipotesi il numero dei "responsabili *privacy*" e il numero dei trattamenti censiti.

Nella precedente versione delle Linee guida (Appendice C) si prevedeva all'interno del criterio "tipologia dei dati trattati" una serie di classi di dati (amministrativi, tecnici, anagrafici semplici, personali sensibili, sanitari, giudiziari) cui era attribuito un "peso specifico" diverso. Nel precedente parere del Garante, il sistema in questione era stato oggetto di una raccomandazione che non solo suggeriva l'utilizzo di una corretta terminologia, ma anche la modifica delle classi di dati nonché del relativo "peso specifico". L'odierno provvedimento non individua i singoli parametri né gli attribuisce un peso specifico; ove dovessero essere ripristinati, è opportuno che si tenga conto delle raccomandazioni del Garante.

RITENUTO

4. La sicurezza dei dati.
Con riferimento agli aspetti più strettamente tecnologici non si segnalano nello schema di Linee guida particolari criticità sotto il profilo della protezione dei dati personali. Nel documento è stata posta attenzione alla sicurezza informatica dei dati e dei sistemi, includendo, altresì, riferimenti alle regole e alle misure previste dal Codice e rinvii a provvedimenti e pubblicazioni del Garante pertinenti agli argomenti discussi (come ad esempio nel caso dell'utilizzo delle tecnologie di *Cloud-computing* per implementare servizi di DR).

Residua, nondimeno, l'esigenza di qualche perfezionamento, per lo più formale, del documento, secondo le modalità di seguito esposte.

4.1. La soppressione del documento programmatico sulla sicurezza.
Rispetto alla precedente versione delle Linee guida, il quadro normativo è cambiato.

Nella precedente versione dell'articolo 34, comma 1-*bis* del Codice, alcuni titolari del trattamento erano tenuti alla redazione del documento programmatico sulla sicurezza.

Successivamente, l'articolo 34, comma 1-*bis* del Codice, che disciplinava appunto il documento programmatico sulla sicurezza (DPS), è stato abrogato dall'articolo 45, comma 1, lett. c), del decreto legge 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Conseguentemente, è necessario espungere dallo schema in esame il riferimento al documento programmatico sulla sicurezza (o DPS), ovunque esso ricorra (vedi pagg. 51, 77, 99, 100 e 101).

4.2. Modifiche formali.

Al fine di utilizzare una corretta terminologia all'interno delle Linee guida, si suggerisce di utilizzare per il decreto legislativo 196 del 2003 l'espressione "Codice in materia di protezione dei dati personali" piuttosto che altre difformi utilizzate nel testo quali "Testo unico in materia di protezione dei dati personali" o "codice della privacy" (vedi pagg. 2, 21, 47, 52, 79, 82, 120, 128 e 129).

Allo stesso modo, si suggerisce di utilizzare l'espressione "Garante per la protezione dei dati personali" piuttosto che ulteriori differenti locuzioni quale "garante privacy" (vedi pagg. 4, 28, 81, 82 e 126), nonché quella di "responsabili del trattamento dei dati" in luogo di "responsabili privacy" (pag. 51).

Per identificare in modo univoco le disposizioni del Codice, si suggerisce, infine:

a) di inserire nella locuzione in cui si indica il "titolo VII del citato DLgs. 196/2003 e s.m.i. che regola il "Trasferimento dei dati all'estero"" le parole "della parte I" tra "VII" e "del" (pag. 82), nonché all'interno della locuzione "nel Titolo VII regola il "Trasferimento dei dati all'estero"" le parole "della parte I" tra "VII" e "regola" (Appendice D.3, pag. 128);
b) di inserire nella locuzione "Titolo IV del citato codice" le parole "della parte I" tra "IV" e "del" (pag. 126).

IL GARANTE

esprime parere favorevole sullo schema di "Linee-guida per il *Disaster Recovery* delle pubbliche amministrazioni", emanate ai sensi dell'articolo 50-*bis*, comma 3, lett. b), del Codice dell'amministrazione digitale, con la seguente osservazione:

a) nello schema di Linee guida sia soppresso il riferimento al documento programmatico sulla sicurezza (o DPS) ovunque esso ricorra (punto 4.1) e siano apportati i perfezionamenti formali indicati al punto 4.2.

Roma, 4 luglio 2013

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia