Provvedimento Garante per la Protezione dei Dati Personali 2 luglio 2015, n. 393
Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche.
Gazzetta Ufficiale 04/8/2015, n. 179

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;
Visto il decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (di seguito Codice);
Visto il decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (di seguito Cad);
Considerate le peculiari caratteristiche delle banche dati delle amministrazioni pubbliche, contraddistinte, in particolare, dall'ingente mole di dati trattati, dalla delicatezza delle informazioni ivi contenute e dalla molteplicità di soggetti autorizzati ad accedervi, nonché l'esigenza di garantire costantemente l'esattezza, l'integrità e la disponibilità dei dati personali ivi contenuti non solo in relazione alle c. d. basi dati di interesse nazionale (art. 60 del Cad), unitamente agli specifici rischi di accesso non autorizzato e di trattamento non consentito;
Ritenuto necessario assoggettare il trattamento dei dati personali effettuato nell'ambito delle predette banche dati all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati o incidenti informatici (accessi abusivi, azione di malware) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione;
Ritenuto, pertanto, che le pubbliche amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 debbano comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati (c.d. data breach) e che tali comunicazioni devono essere redatte secondo lo schema riportato nell'Allegato 1 al presente provvedimento e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo:
- databreach.pa@pec.gpdp.it;
Vista, inoltre, la nuova formulazione dell'art. 58, comma 2, del Cad, così come modificato dall'art. 24-quinquies, comma 1, decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114, in vigore dal 19 agosto 2014, la quale ha previsto che «le pubbliche amministrazioni comunicano tra loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'art. 72, comma 1, lettera e). L'Agenzia per l'Italia digitale, sentiti il Garante per la protezione dei dati personali e le amministrazioni interessate alla comunicazione telematica, definisce entro novanta giorni gli standard di comunicazione e le regole tecniche a cui le pubbliche amministrazioni devono conformarsi»;
Considerato che tale modifica ha superato, quindi, il pregresso impianto normativo relativo all'accessibilità telematica ai dati delle pubbliche amministrazioni, fondato su «apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti» (testo previgente dell'art. 58, comma 2 del Cad);
Considerato, altresì, che il Garante, nell'ambito del parere del 4 luglio 2013 (doc. web n. 2574977) sulle apposite linee guida dell'Agenzia per l'Italia digitale (di seguito Agid) per la stipula delle predette convenzioni aperte aveva prescritto alle amministrazioni destinatarie delle stesse l'adozione di specifiche misure tecniche e organizzative;
Considerato che nel trattamento di dati personali l'erogatore (amministrazione titolare del trattamento dei dati personali che mette a disposizione i relativi servizi di accesso) e il fruitore (amministrazione richiedente che accede in qualità di autonomo titolare ai dati personali resi disponibili dall'erogatore) sono chiamati a rispettare il Codice con particolare riferimento ai presupposti che legittimano i flussi di dati e agli adempimenti in materia di misure di sicurezza;
Ritenuto necessario, pertanto, nelle more della definizione da parte dell'Agid dei suindicati «standard di comunicazione e le regole tecniche», confermare le specifiche misure tecniche e organizzative già individuate, prescrivendo nuovamente l'adozione delle stesse - riportate nell'Allegato 2 al presente

provvedimento - al fine di ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento ai sensi dell'art. 31 del Codice, salvo che le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti;
Rilevato che le misure necessarie individuate nell'Allegato 2, adeguate al nuovo contenuto del citato art. 58, comma 2, nella sostanza risultano equivalenti a quelle prescritte dal Garante nell'ambito del predetto parere sulle linee guida dell'Agid del 4 luglio 2013;
Ritenuto, pertanto, che le convenzioni già predisposte dalle amministrazioni nel rispetto del richiamato parere del Garante, anche al fine di garantire il rispetto del principio di semplificazione, debbano ritenersi conformi alle misure necessarie individuate nell'Allegato 2 al presente provvedimento;
Ritenuto, invece, che laddove siano state previste modalità di accesso ai dati personali ai sensi della nuova formulazione del predetto art. 58, comma 2 del Cad, non conformi alle misure già individuate dal Garante nel citato provvedimento del 4 luglio 2013, le misure previste nell'Allegato 2 debbano essere adottate dalle amministrazioni interessate entro e non oltre il 31 dicembre 2015;
Rilevato, infine, che la mancata comunicazione al Garante dei c.d. data breach, nonché la mancata adozione delle misure necessarie individuate nell'Allegato 2 al presente provvedimento nei suesposti termini e modalità, configurano un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter del Codice;
Vista la documentazioni 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;

Tutto ciò premesso il Garante:

1. Ai sensi dell'art. 154, comma 1, lett. c), del Codice, prescrive che le pubbliche amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni debbano essere redatte secondo lo schema riportato nell'Allegato 1 al presente provvedimento e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.pa@pec.gpdp.it;
2. Ai sensi dell'art. 154, comma 1, lett. c), del Codice, nelle more della definizione degli «standard di comunicazione e le regole tecniche» da parte dell'Agid ai sensi dell'art. 58, comma 2, del Cad, prescrive alle pubbliche amministrazioni che intendano mettere a disposizione gli accessi alle proprie banche dati alle altre amministrazioni che ne abbiano diritto mediante la cooperazione applicativa di cui all'art. 72, comma 1, lettera e) del Cad l'adozione delle misure necessarie individuate nell'Allegato 2 al presente provvedimento, salvo che le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti; laddove siano già state previste modalità di accesso ai sensi della nuova formulazione del predetto art. 58, comma 2 del Cad, non conformi alle misure già individuate dal Garante nel provvedimento del 4 luglio 2013, prescrive che le misure necessarie previste nell'Allegato 2 siano adottate dalle amministrazioni interessate entro e non oltre il 31 dicembre 2015;
3. Ai sensi dell'art. 143, comma 2, del Codice dispone la trasmissione di copia del presente provvedimento al Ministero della giustizia - Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 2 luglio 2015