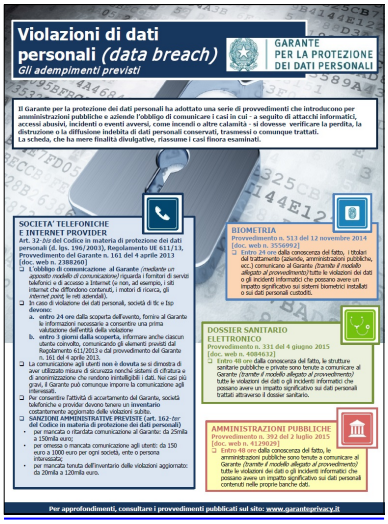
Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013 [2388260]



INFOGRAFICA - VIOLAZIONI DI DATI PERSONALI. GLI ADEMPIMENTI PREVISTI

VEDI ANCHE Comunicato stampa del 26 aprile 2013

[Modello destinato ai fornitori di servizi di comunicazione elettronica per la comunicazione dei casi di violazione dei dati personali (data breach)](*)

VEDI PROVVEDIMENTO DEL 30 LUGLIO 2019 SULLA NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

[doc. web n. 2388260]

Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013

(Pubblicato sulla Gazzetta Ufficiale n. 97 del 26 aprile 2013)

Registro dei provvedimenti
n. 161 del 4 aprile 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 dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice") e, in particolare, gli

artt. 32 e 32-bis;

VISTA la precedente deliberazione del Garante recante "Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" (Del. n. 221 del 26 luglio 2012, in G.U. n. 183 del 7 agosto 2012);

TENUTO CONTO delle risultanze dei contributi pervenuti al Garante dai principali fornitori di servizi di comunicazione elettronica, nonché da alcune associazioni di studio e ricerca del settore, che hanno partecipato alla consultazione pubblica avviata con la richiamata deliberazione del 26 luglio 2012;

CONSIDERATI i primi casi di violazione di dati personali verificatisi dall´entrata in vigore della nuova disciplina e comunicati al Garante dai fornitori in ottemperanza a quanto previsto dall´art. 32-bis, comma 1, del Codice;

RITENUTO necessario adottare, ai sensi dell´art. 32-bis, comma 6, del Codice, un provvedimento generale che sostituisce le suindicate Linee guida al fine di fornire orientamenti e istruzioni in relazione alle circostanze in cui il fornitore ha l´obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione;

VISTE le osservazioni dell´Ufficio, formulate dal segretario generale ai sensi dell´art. 15 del regolamento n. 1/2000;

RELATORE la dott.ssa Augusta Iannini;

PREMESSA

1. Considerazioni preliminari.

La direttiva 2002/58/Ce (c.d. direttiva e-Privacy) afferma che i fornitori di servizi di comunicazione elettronica devono adottare "appropriate misure tecniche e organizzative" per assicurare "un livello di sicurezza adeguato al rischio esistente" (art. 4, comma 1). Nella direttiva 2009/136/Ce (che ha modificato la direttiva 2002/58/Ce) si è tenuto conto, in particolare, del fatto che un evento che coinvolga i dati personali, se non trattato in modo adeguato e tempestivo, può provocare un grave danno economico e sociale al contraente (o alle altre persone interessate), tra cui l´usurpazione d´identità (cfr. considerando 61).

Con il recepimento delle suindicate previsioni tramite il decreto legislativo 28 maggio 2012, n. 69, con il quale il Governo ha dato attuazione alla delega prevista nell´art. 9 della legge comunitaria del 2010 (legge 15 dicembre 2011, n. 217, pubblicata in G.U. 2 gennaio 2012, n. 1), i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare senza indebiti ritardi al Garante e, in alcuni casi, al contraente o ad altre persone interessate, l´occorrenza dei predetti eventi, qualificati come "violazioni di dati personali".

2. Quadro normativo.

Come sopra accennato, il decreto legislativo 28 maggio 2012, n. 69 ha apportato significative e numerose modifiche al Codice, introducendo, per quanto di specifico interesse, la nuova disciplina concernente la gestione delle suindicate violazioni di sicurezza nel settore delle comunicazioni elettroniche.

È stata così introdotta la definizione di "violazione di dati personali", intesa come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l´accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico" (art. 4, comma 3, lett. g-bis), del Codice).

Si tratta di una definizione da un lato molto ampia, in quanto comprende qualunque evento metta a rischio, anche in maniera del tutto accidentale, i dati trattati nell´ambito dei servizi di comunicazione elettronica, e dall´altro volta a delimitare il contesto (quello, appunto, dei servizi di comunicazione elettronica accessibili al pubblico), nonché l´ambito soggettivo (quello dei fornitori di tali servizi), nel quale opera la nuova disciplina.

In quest´ottica vanno lette anche le modifiche all´art. 32 del Codice, ora espressamente rubricato "Obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico" e che impone al fornitore di adottare, anche attraverso altri soggetti cui

sia affidata l´erogazione del servizio, "misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi e per gli adempimenti di cui all´articolo 32-bis".

Il legislatore comunitario è peraltro consapevole del fatto che l´interesse degli utenti ad essere informati sulle violazioni di sicurezza che coinvolgono i loro dati personali non si limita al settore delle comunicazioni elettroniche. Ed infatti, le proposte di riforma della legislazione comunitaria in materia di protezione dei dati (cfr. schema di Regolamento presentato dalla Commissione europea il 25 gennaio 2012, attualmente all´esame del Parlamento e del Consiglio) prevedono un´estensione generalizzata dell´obbligo di notifica delle violazioni dei dati personali a tutti i titolari pubblici e privati (v. anche considerando 59, direttiva 2009/136/Ce).

In alcuni Stati membri del resto sono già in vigore disposizioni che prevedono una platea più ampia di soggetti che effettuano tale notifica (es. in Irlanda); in tal senso, peraltro, si è espresso anche il Gruppo dei Garanti europei (c.d. "Gruppo Art. 29") nel documento n. 01/2011, adottato il 5 aprile 2011.

L´art. 32-bis citato introduce poi nel Codice la disciplina degli "Adempimenti conseguenti ad una violazione di dati personali" e sancisce l´obbligo, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, di comunicare senza indebiti ritardi al Garante la violazione di dati personali da essi detenuti. Nei casi in cui dalla violazione possa derivare pregiudizio ai dati personali o alla riservatezza di un contraente o di altra persona, il fornitore dovrà comunicare l´avvenuta violazione anche a tali soggetti (art. 32-bis, comma 2).

Tale seconda comunicazione ferma restando la difficoltà, sulla quale si tornerà in seguito, di delimitare i casi nei quali la violazione possa arrecare pregiudizio al contraente o ad altre persone interessate, potendo tale rischio dirsi in astratto sempre sussistente non è dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure "che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate al momento della violazione" (art. 32-bis, comma 3). Il Garante, considerate le presumibili ripercussioni negative della violazione, può comunque obbligare il fornitore ad effettuare la predetta comunicazione, ove lo stesso non vi abbia già provveduto (comma 4).

3. Ambito soggettivo.

Come si è già accennato, la nuova disciplina concernente gli obblighi di comunicazione al Garante e alle persone interessate non riguarda la totalità dei titolari dei trattamenti, ossia dei soggetti, pubblici o privati, che detengono e trattano dati personali in funzione della propria attività.

I nuovi adempimenti gravano, infatti, esclusivamente sui fornitori di servizi di comunicazione elettronica accessibili al pubblico (di seguito, "fornitori") e, quindi, su quei soggetti che mettono a disposizione del pubblico, su reti pubbliche di comunicazione, servizi consistenti, esclusivamente o prevalentemente, "nella trasmissione di segnali su reti di comunicazioni elettroniche" (art. 4, comma 2, lett. d) ed e), del Codice).

I medesimi adempimenti sono inoltre connessi alla particolare attività di fornitura dei predetti servizi, quale ad esempio il servizio telefonico o quello di accesso a Internet. Ciò significa che se la violazione riguarda una banca dati del fornitore che non attiene in maniera specifica al servizio offerto dallo stesso, ma ad una qualunque delle altre attività che svolge, ad esempio alla gestione del personale o alla contabilità, l´obbligo di comunicazione non vige.

Al riguardo, anche al fine di individuare i soggetti interessati dalla nuova disciplina, si rinvia alle indicazioni fornite dal Garante con il provvedimento relativo alla "Sicurezza dei dati di traffico telefonico e telematico" (provv. del 17 gennaio 2008, pubblicato in G.U. n. 30 del 5 febbraio 2008, come modificato e integrato dal provvedimento del 24 luglio 2008, pubblicato in G.U. n. 189 del 13 agosto 2008), in quanto vi è una sostanziale identità dei titolari tenuti alla conservazione ex art. 132 del Codice, nonché all´adozione delle misure ivi prescritte con i destinatari della nuova disciplina ex art. 32-bis.

In tale provvedimento, infatti, è stato evidenziato che "fornitori di servizi di comunicazione elettronica accessibili al pubblico" sono quei soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall´assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione (cfr. anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica -c.d. direttiva quadro- e d.lg. n. 259/2003 recante il Codice delle comunicazioni elettroniche).

Al contrario non rientrano tra tali soggetti:

- coloro che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nella definizione generale di "servizi di comunicazione elettronica", non possono essere infatti considerati come "accessibili al pubblico";

- i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale;

- i gestori dei siti Internet che diffondono contenuti sulla rete (c.d. "content provider"). Essi non sono, infatti, fornitori di un "servizio di comunicazione elettronica" come definito dall´art. 4, comma 2, lett. e) del Codice. Tale norma, infatti, nel rinviare, per i casi di esclusione, all´art. 2, lett. c) della direttiva 2002/21/Ce cit., esclude essa stessa i "servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica […]". Qualora tali soggetti offrano anche il servizio di posta elettronica, limitatamente alla gestione dei dati personali relativi allo stesso, rientrano viceversa nel campo di applicazione della nuova disciplina;

- i gestori di motori di ricerca, salvo l´eventuale componente di trasmissione dati.

Discorso a parte va fatto per i servizi di Mobile Payment eventualmente offerti dal fornitore ai propri utenti. Si tratta di servizi che consentono di effettuare pagamenti o trasferimenti di denaro tramite telefono mobile, che molti fornitori stanno implementando a seguito del recepimento della direttiva n. 2007/64/Ce (la c.d. PSD, "Payment Service Directive") ad opera del d.lgs. 27 gennaio 2010, n. 11.

Più specificamente, il pagamento del bene o servizio acquistato avviene o mediante carta di credito su disposizione inviata per il tramite del telefono mobile in presenza di apposito lettore POS (c.d. modalità "proximity"), oppure con addebito e conseguente decurtazione del costo dal credito telefonico, per i clienti dotati di una carta ricaricabile, e con addebito sul conto telefonico, per i clienti in abbonamento (c.d. modalità "remote").

In quest´ultimo caso, i dati di pagamento dei clienti sono strettamente connessi a quelli di traffico telefonico degli stessi; si ritiene pertanto che anche per le violazioni riguardanti tali servizi il fornitore sia tenuto agli obblighi di cui all´art. 32-bis del Codice.

3.1. Servizi erogati tramite altri soggetti.

La nuova normativa prende espressamente in considerazione l´ipotesi in cui il fornitore affidi l´erogazione del servizio di comunicazione elettronica ad altri soggetti. In particolare, l´art. 32-bis, comma 8, prevede che, in questi casi, i soggetti esterni affidatari dell´erogazione del servizio siano tenuti a comunicare "senza indebito ritardo al fornitore tutti gli eventi e le informazioni necessarie a consentire a quest´ultimo di effettuare gli adempimenti" in materia di violazione dei dati personali.

Si tratta di una disposizione che riguarda la particolare situazione che vede coinvolti i fornitori di comunicazione elettronica "tradizionali" e, ad esempio, i c.d. operatori virtuali di rete mobile (Mobile Virtual Network Operator, MVNO), ossia le società che forniscono servizi di telefonia mobile senza possedere alcuna licenza per il relativo spettro radio né tutte le infrastrutture necessarie per fornire tali servizi e che utilizzano a tale scopo una parte dell´infrastruttura di uno o più operatori mobili reali (MNO).

I MVNO sono dotati di archi di numerazione telefonica propri e quindi di proprie SIM card, possono gestire in proprio le funzioni di commutazione e di trasporto nonché la base dati di registrazione degli utenti mobili. Sono, quindi, completamente autonomi nella relazione con i clienti, i quali non hanno alcun rapporto diretto con l´operatore di rete mobile e stipulano un unico contratto, appunto, con il MVNO.

Da ciò emerge, pertanto, come gli obblighi di comunicazione derivanti da eventuali violazioni di dati personali dei clienti (o di altre persone interessate) incombano sul MVNO, l´unico a conoscere, nella maggior parte dei casi, l´identità dei clienti stessi. E tuttavia, in ragione del fatto che, come detto, il servizio viene materialmente erogato congiuntamente con il MNO e che, quindi, possono essere coinvolti sistemi dei quali dispone soltanto quest´ultimo, è necessario che tale soggetto renda noti tutti gli eventi e le informazioni concernenti l´avvenuta violazione all´operatore virtuale, in modo tale che questo possa adempiere ai propri obblighi nei confronti del Garante e, eventualmente, dei clienti.

Al riguardo, si rinvia alle definizioni contenute nella Delibera dell´Autorità per le garanzie nelle comunicazioni n. 544/00/CONS, "Condizioni regolamentari relative all´ingresso di nuovi operatori nel mercato dei sistemi radiomobili" (pubblicata in G.U. n. 183 del 7 agosto 2000).

Un altro caso rientrante nella previsione di cui al comma 8 è quello nel quale il fornitore del servizio di comunicazione elettronica, pur potendosi definire "tradizionale", affidi in tutto o in parte la materiale erogazione del servizio stesso a soggetti terzi, che abbiano le infrastrutture a ciò necessarie, ad esempio per ragioni di ottimizzazione dei costi.

Ferma restando la necessità che in tali ipotesi i soggetti coinvolti configurino correttamente i rispettivi ruoli in termini di titolare e responsabile del trattamento, l´eventuale violazione dei dati personali trattati nell´ambito dei sistemi affidati dal fornitore al soggetto terzo, dovrà essere da questo necessariamente comunicata al fornitore stesso entro 24 ore dall´avvenuta conoscenza della violazione, il quale potrà poi comunicare a sua volta la violazione al Garante e, se occorre, al contraente o ad altra persona interessata, come riportato al punto 5.

4. Gestione della sicurezza e delle violazioni.

L´art. 32 del Codice (come modificato dal d.lg. n. 69/2012 in attuazione di quanto previsto dall´art. 4 della direttiva 2002/58/Ce) prevede che i soggetti che operano sulle reti di comunicazione elettronica debbano garantire "che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati" (cfr. comma 1-bis) e che le misure tecniche e organizzative, che il fornitore di comunicazione elettronica deve adottare, siano adeguate al rischio esistente, garantiscano la protezione dei dati archiviati o trasmessi da una serie di eventi espressamente indicati (distruzione, perdita, alterazione, anche accidentali, archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti) e assicurino l´attuazione di una "politica di sicurezza" (cfr. comma 1-ter).

Il nuovo art. 32, comma 3, infine, impone al fornitore di informare i contraenti, il Garante, l´Agcom e, ove possibile, gli utenti, dell´esistenza di "un particolare rischio di violazione della sicurezza della rete", indicando, quando il rischio è al di fuori dell´ambito di applicazione delle suindicate misure, tutti i possibili rimedi e i relativi costi presumibili.

Tali previsioni indicano chiaramente come i fornitori siano tenuti ad organizzarsi al proprio interno al fine di garantire un elevato livello di sicurezza dei dati detenuti e gestire in maniera strutturata e tramite procedure e interventi definiti a priori, le eventuali violazioni di dati personali che dovessero accadere.

Come dichiarato anche dall´ENISA nelle sue recenti Raccomandazioni (disponibili all´indirizzo http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech), la gestione del rischio, in primo luogo, e delle violazioni di dati personali, qualora dovessero verificarsi, non può essere affidata dai fornitori a un´attività estemporanea. Essa richiede la predisposizione di un idoneo piano, nel quale dovrà essere individuata una serie di misure tecniche e organizzative di livello commisurato al tipo di minaccia, in grado di garantire risposte tempestive, efficaci e adeguate all´entità della violazione.

Quanto all´individuazione delle misure minime di sicurezza propriamente dette ossia quelle alle quali la legge riconduce sanzioni di carattere anche penale ex art. 169 del Codice si richiama l´art. 33 del Codice e le specifiche previsioni contenute nel Disciplinare tecnico in materia di misure minime di sicurezza, di cui all´Allegato B (in particolare quelle relative ai trattamenti svolti con strumenti elettronici), la cui adozione è peraltro obbligatoria per qualunque titolare del trattamento.

4.1. Analisi dei rischi.

Al fine di ottemperare agli obblighi di cui all´art. 32 del Codice, è necessario che i fornitori effettuino una preliminare ricognizione dell´insieme dei dati personali trattati e dei rischi ai quali gli stessi vanno incontro.

È necessario, quindi, che ciascun fornitore identifichi e attribuisca un valore ai differenti dati personali che detiene e ai pericoli cui gli stessi sono esposti, individuando la propria soglia di accettazione dei rischi e fissando le opportune strategie di gestione. Il fornitore è anche tenuto a individuare delle soglie di rischio, ad esempio in base a livello basso, medio e alto, in ragione delle quali decidere non solo quali misure adottare per garantire un´idonea protezione dei dati detenuti, ma anche se effettuare la comunicazione al contraente o alle altre persone interessate.

Tale preliminare ricognizione consentirà ai fornitori di predisporre misure di sicurezza volte sia a prevenire i possibili eventi avversi, sia a intervenire nel momento in cui gli stessi dovessero comunque -nonostante le misure adottate verificarsi.

Si tratta di valutazioni sostanzialmente analoghe a quelle che i fornitori, sino al 10 febbraio 2012, erano tenuti ad effettuare ai fini della redazione del Documento programmatico sulla sicurezza, misura minima prevista dalla regola 19 del richiamato Disciplinare tecnico, abrogata dall´art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5 (convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35).

4.2. Adozione di adeguate misure di sicurezza.

L´analisi dei rischi sopra indicata è alla base della predisposizione, da parte dei fornitori, delle misure di sicurezza "adeguate al rischio esistente", richiamate dal nuovo art. 32, comma 1, del Codice, nonché dell´individuazione di quelle maggiormente in grado di porre rimedio alla violazione eventualmente verificatasi, le quali peraltro debbono essere descritte al Garante nella comunicazione, come previsto dall´art. 32-bis, comma 5, del Codice.

Si suggeriscono in particolare, le seguenti misure in grado di garantire un livello minimo comune di sicurezza, che vanno ad aggiungersi a quelle prescritte con il citato provvedimento relativo alla "Sicurezza dei dati di traffico telefonico e telematico" del 17 gennaio 2008, nonché con quello relativo alle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 (pubblicato in G.U. n. 300 del 24 dicembre 2008 e modificato in base al provvedimento del 25 giugno 2009):

1. rendere i dati trattati immediatamente non disponibili per ulteriori elaborazioni da parte di sistemi informativi al termine delle attività svolte e nelle quali gli stessi sono coinvolti, provvedendo alla loro cancellazione o trasformazione in forma anonima in tempi tecnicamente compatibili con l´esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (backup e disaster recovery), anche con il ricorso a tecnologie crittografiche o di anonimizzazione;

2. porre particolare attenzione ai dispositivi portatili, predisponendo specifiche misure di sicurezza in grado di mitigare il rischio connesso alla portabilità dell´apparato, e di assicurare agli stessi un livello di sicurezza analogo a quello applicato agli altri dispositivi informatici, in considerazione del fatto che molto spesso le violazioni della sicurezza riguardano i dispositivi mobili utilizzati da dipendenti e collaboratori dei fornitori al di fuori degli uffici delle aziende.

5. Comunicazione al Garante: tempi e contenuto.

La predisposizione da parte dei fornitori di un idoneo piano di gestione delle violazioni sulla base di un´accurata analisi dei rischi è necessaria per poter adempiere correttamente anche all´obbligo di comunicazione al Garante previsto dall´art. 32-bis. Tale disposizione stabilisce infatti che il fornitore debba comunicare la violazione dei dati personali al Garante "senza indebiti ritardi", ossia nel momento in cui lo stesso ne viene a conoscenza.

Stante l´importanza della tempestività della comunicazione al Garante, ma considerando anche la complessità e il numero dei sistemi in uso presso i fornitori, nonché dei dati che detengono, si ritiene che tali soggetti nelle situazioni più articolate possano, in un primo momento, limitarsi a fornire all´Autorità sommarie informazioni in relazione alla violazione verificatasi, purché ciò avvenga immediatamente dopo l´avvenuta conoscenza della stessa, integrando poi la comunicazione in un momento successivo.

Tali sommarie informazioni devono in ogni caso consentire all´Autorità di effettuare una prima valutazione dell´entità della violazione e quindi, affinché la comunicazione possa essere considerata come validamente effettuata, le stesse devono comprendere:

- i dati identificativi del fornitore;
- una breve descrizione della violazione;
- l´indicazione della data anche presunta della violazione e del momento della sua scoperta;
- l´indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di

smarrimento di dispositivi o di supporti portatili;

• l´indicazione della natura e della tipologia dei dati anche solo presumibilmente coinvolti;

• una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Si ritengono congrui, quali termini entro i quali provvedere alla comunicazione, quello di 24 ore dall´avvenuta conoscenza della violazione per la prima sommaria comunicazione, e quello di 3 giorni dalla stessa per la comunicazione dettagliata.

Per agevolare l´adempimento, è stato predisposto un modello di comunicazione da inviare al Garante, disponibile on line sul sito dell´Autorità e idoneo alla raccolta delle informazioni sulla violazione nonché al loro successivo trattamento con strumenti informatici da parte del Garante (Allegato 1).

Quanto al contenuto della comunicazione, l´art. 32-bis, comma 5, del Codice prevede che essa, oltre alla descrizione della natura della violazione, all´indicazione dei punti di contatto presso cui ottenere maggiori informazioni e all´elenco delle misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione (elementi da inserire anche nell´eventuale comunicazione ai soggetti interessati), descriva le conseguenze della violazione e le misure proposte o adottate dal fornitore per porvi rimedio.

Laddove la scoperta della violazione non sia stata contestuale al verificarsi dell´evento, si ritiene necessario che nella suindicata comunicazione vengano puntualmente indicate le ragioni che non hanno consentito l´immediata rilevazione dell´evento medesimo e le misure adottate o che si intende adottare affinché ciò non si ripeta.

Qualora, all´esito delle verifiche effettuate dal fornitore successivamente alla prima sommaria comunicazione, non dovessero emergere ulteriori elementi, il fornitore dovrà comunicare al Garante le modalità con le quali ha posto rimedio alla violazione e le misure adottate per prevenire ulteriori violazioni della medesima specie.

In sostanza, è necessario che dalla comunicazione emergano gli elementi dai quali l´Autorità possa valutare compiutamente la gravità dell´evento verificatosi, anche in ragione del numero dei soggetti coinvolti e della quantità e qualità dei dati colpiti, l´entità del danno cagionato e le misure adottate per ridurlo. Ciò, al fine di intervenire con le prescrizioni che si rendessero necessarie, compresa quella di comunicare l´avvenuta violazione ai contraenti o alle altre persone interessate.

Parimenti importante, al fine di consentire all´Autorità di svolgere eventuali accertamenti, risulta l´indicazione, nella comunicazione, dei sistemi applicativi colpiti dalla violazione, nonché l´ubicazione fisica dei sistemi di elaborazione impiegati nel trattamento.

L´obbligo di comunicare l´avvenuta violazione al Garante ed eventualmente al contraente (o ad altra persona interessata) sussiste, ovviamente, anche qualora l´evento abbia interessato dispositivi mobili e indipendentemente dal fatto che sugli stessi siano installati sistemi di protezione dei dati. Anche per tali dispositivi (come si vedrà nel prosieguo) l´unica ipotesi in cui il fornitore può esimersi dalla comunicazione al contraente (o ad altra persona interessata) è quella in cui i dati in essi contenuti o tramite gli stessi accessibili siano stati resi inintelligibili.

L´Autorità si riserva di intervenire nuovamente in merito ai tempi e al contenuto della comunicazione al Garante qualora nell´emanando Regolamento della Commissione relativo alle misure applicabili alla comunicazione delle violazioni di dati personali nell´ambito della Direttiva 2002/58/Ce sulla privacy e le comunicazioni elettroniche dovesse emergere un differente orientamento al riguardo.

6. Inventario delle violazioni di dati personali.

Al medesimo scopo, quello cioè di consentire al Garante di svolgere il proprio compito di controllo sul rispetto, da parte dei fornitori, delle disposizioni in materia di violazione dei dati personali, è finalizzata la previsione relativa alla tenuta di un inventario aggiornato delle violazioni, di cui all´art. 32-bis, comma 7, del Codice (cfr. anche considerando 58, direttiva 136/2009/Ce).

In tale inventario, i fornitori devono inserire tutte (e soltanto) le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate le violazioni, le conseguenze che le stesse hanno avuto e i provvedimenti adottati per porvi rimedio.

Proprio per consentire il raggiungimento delle finalità dichiarate dalla disposizione in questione, è opportuno che l´inventario tenga traccia delle varie fasi con le quali il fornitore ha gestito l´incidente/evento, dalla sua scoperta alla sua risoluzione/conclusione, ivi comprese le comunicazioni inviate al Garante e al contraente e/o ad altra persona. In tal modo, l´inventario potrà costituire per i fornitori anche un valido strumento per un´analisi statistica delle diverse tipologie di violazioni che hanno interessato i servizi offerti e per l´adozione di misure atte a migliorare la politica di sicurezza dell´azienda.

L´inventario, pertanto, dovrà essere continuamente aggiornato dai fornitori e messo a disposizione del Garante, qualora l´Autorità chieda di accedervi. In ogni caso, anche ai fini dell´applicazione delle sanzioni previste, i fornitori dovranno registrare nell´inventario il data breach che li ha coinvolti contestualmente alla comunicazione al Garante indicata al punto 5, avendo cura poi di inserire tempestivamente gli elementi che dovessero emergere successivamente, anche all´esito di ulteriori verifiche.

Dovranno, inoltre, essere adottate dal fornitore idonee misure atte a garantire l´integrità e l´immodificabilità delle registrazioni in esso contenute.

7. Comunicazione al contraente o ad altre persone.

Qualora si verifichi una violazione di dati personali e dalla stessa possa derivare un pregiudizio ai dati personali o alla riservatezza di un contraente o di altre persone, ossia dei soggetti ai quali si riferiscono i dati violati, oltre alla comunicazione al Garante, i fornitori sono tenuti a comunicare l´avvenuta violazione, senza ritardo, anche a tali soggetti (art. 32-bis, comma 2, del Codice).

Per il contenuto di tale comunicazione, si rinvia al punto 5.

In questo caso, si ritiene che il fornitore debba procedere alla suindicata comunicazione non oltre il termine di 3 giorni dall´avvenuta conoscenza della violazione. Il fornitore potrà poi scegliere il canale di comunicazione che riterrà più idoneo, tenendo conto di quanto indicato nel successivo punto 7.2.

Anche in ragione delle indicazioni provenienti dalla Commissione, si ritiene che in circostanze eccezionali, qualora la comunicazione al contraente o ad altre persone possa pregiudicare lo svolgimento delle verifiche sul data breach, il Garante possa autorizzare il fornitore a ritardare la medesima comunicazione per il tempo strettamente necessario al completamento delle stesse.

La predetta comunicazione non è dovuta se il fornitore è in grado di dimostrare al Garante di aver applicato ai dati oggetto della violazione misure tecnologiche di protezione che li hanno resi inintelligibili a chiunque non sia autorizzato ad accedervi (cfr. art. 32-bis, comma 3, del Codice).

La misura dell´inintelligibilità dei dati violati non riguarda naturalmente l´ipotesi in cui la "violazione della sicurezza" (cfr. art. 4, comma 3, lett. g-bis), del Codice) abbia comportato la distruzione o la perdita dei dati personali dei contraenti. In tale evenienza, infatti, la violazione riguarda profili della sicurezza diversi dalla confidenzialità dei dati, determinando il venir meno dell´integrità e/o della disponibilità degli stessi da parte degli interessati, ai quali potrebbe pertanto rendersi necessario comunicare l´accaduto.

In ogni caso, in ragione dell´entità del possibile pregiudizio per gli interessati, devono essere sempre comunicate immediatamente ai contraenti le violazioni che riguardano le credenziali di autenticazione (nome utente e password, ancorché quest´ultima sia cifrata o sottoposta a funzioni di hashing) o le chiavi di cifratura utilizzate dai contraenti medesimi.

7.1. Inintelligibilità dei dati.

A giudizio dell´Autorità, si considerano inintelligibili i dati che, ad esempio:

a. siano stati cifrati in modo sicuro attraverso un algoritmo standardizzato, o mediante l´impiego di schemi di cifratura a chiave simmetrica o pubblica noti in letteratura, purché la chiave di decifrazione sia di adeguata lunghezza (espressa in numero di bit), sia stata predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

b. siano stati sostituiti da un valore di hash calcolato attraverso una funzione crittografica di hashing a chiave, purché la chiave utilizzata per effettuare lo hashing dei dati sia di adeguata lunghezza (espressa in numero di bit), sia stata

predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

c. siano stati resi anonimi con procedure tali da non consentire la reidentificazione degli interessati cui si riferiscono da parte di soggetti non legittimati al loro trattamento, anche mediante il ricorso ad altre fonti informative disponibili presso il titolare o pubbliche.

In ragione del fatto che, astrattamente, il rischio che una violazione di dati personali arrechi pregiudizio ai dati stessi o alla riservatezza dei soggetti ai quali essi si riferiscono è sempre sussistente, non è certamente semplice definire a priori in quali casi il fornitore possa esimersi dall´effettuare la comunicazione della violazione al contraente o alle altre persone interessate.

L´art. 32-bis, comma 4, del Codice prevede comunque che, ove il fornitore non vi abbia provveduto, il Garante, considerate le presumibili ripercussioni negative della violazione, può obbligare lo stesso ad effettuare la comunicazione al contraente o ad altra persona interessata. È evidente che tale possibilità prescinde dal fatto che il fornitore abbia reso inintelligibili i dati violati: tale evenienza riduce, non fa venir meno, il rischio che i dati violati siano comunque decifrabili e che, pertanto, il Garante imponga di effettuare comunque la comunicazione.

Da quanto detto, risulta di tutta evidenza la necessità che il fornitore dia conto, nella comunicazione al Garante, della politica di sicurezza attuata e che descriva anche le conseguenze della violazione verificatasi e le misure proposte o adottate per porvi rimedio, in tal modo consentendo all´Autorità di fare le proprie valutazioni e dare eventuali prescrizioni.

7.2. Canale per la comunicazione al contraente o ad altre persone.

Ciascun fornitore dovrà valutare quale sia il canale di comunicazione che consente di raggiungere più facilmente e tempestivamente i soggetti i cui dati sono interessati dalla violazione. E ciò, sia con riguardo ai contraenti, sia, soprattutto, con riferimento a quelle persone che non sono clienti del fornitore, ma che pure sono state coinvolte dalla violazione e alle quali il medesimo fornitore potrà rivolgere una comunicazione diretta laddove disponga dei relativi dati personali di contatto senza necessità di ulteriore raccolta di informazioni.

Quando in determinate circostanze non si sia proceduto alla comunicazione individuale - modalità senz´altro da preferire - soprattutto con riferimento ai soggetti da ultimo indicati, ma anche in relazione ai clienti del fornitore, nei casi in cui sia coinvolto un numero molto elevato di contraenti, si ritiene che il medesimo fornitore possa più facilmente raggiungere lo scopo previsto dalla normativa - informare senza ritardo i soggetti i cui dati sono coinvolti dalla violazione - tramite forme di comunicazione diverse da quella ad personam.

Si ritiene, cioè, che in alcuni casi siano più utili forme di comunicazione di carattere pubblico, quali la diffusione di avvisi su quotidiani, anche on line, oppure per mezzo di emittenti radiofoniche, anche locali. Tali forme alternative di comunicazione ai contraenti o alle altre persone coinvolte dalla violazione vanno ovviamente realizzate anch´esse entro il più breve lasso di tempo e, comunque, entro il termine di 3 giorni indicato ai punti 5 e 7.

7.3. Valutazione del rischio che richiede la comunicazione al contraente o ad altre persone.

Come si è detto, è necessario che il fornitore effettui delle valutazioni per decidere quali misure adottare per ridurre il rischio, attenuare il danno qualora si verifichi la violazione e decidere se comunicare al contraente e/o alle altre persone, consentendo loro, così, di adottare le precauzioni necessarie.

Tali valutazioni dovrebbero essere svolte sulla base di criteri determinati e comuni a tutti i fornitori, in modo tale da porre in campo scelte ponderate e confrontabili. Potrebbero soccorrere, ai fini della suindicata valutazione, innanzitutto elementi quali la quantità e la qualità dei dati coinvolti nella violazione.

A titolo meramente esemplificativo, una violazione che riguardi un solo dato personale o, anche, più dati personali, non sensibili, di un solo contraente ferma restando la necessità che il fornitore adotti tutte le misure in grado di ridurre il danno potrebbe non dover essere necessariamente comunicata allo stesso ai sensi dell´art. 32-bis, comma 2.

Parimenti importante e, dunque, da considerare nella valutazione del rischio, è la "attualità" dei dati detenuti, ossia il tempo trascorso dall´acquisizione dei dati stessi e dal loro inserimento nei database del fornitore. Dati più recenti potrebbero infatti destare maggiore interesse per eventuali malintenzionati in quanto è più alta la probabilità che essi esprimano in modo attendibile uno "stato" o una specifica condizione (economica, di salute, abitativa ecc.) in cui si trova l´interessato al momento dell´avvenuta violazione.

Potrebbe essere utile poi, per decidere se comunicare o meno la violazione agli interessati, considerare gli effetti della violazione stessa e ritenere sussistente il pregiudizio per i dati o la vita privata del contraente o di altra persona quando la violazione "implica, ad esempio, il furto o l´usurpazione d´identità, il danno fisico, l´umiliazione grave o il danno alla reputazione in relazione con la fornitura di servizi di comunicazione" (cfr. considerando 61, direttiva 2009/136/Ce).

Per giungere a valori uniformi e comparabili, i fornitori dovrebbero affrontare la valutazione del rischio anche con un approccio di tipo quantitativo, individuando in ragione dei succitati attributi dei dati coinvolti nella violazione (qualità, quantità, attualità, ecc.), specifiche metriche in grado di rappresentare gli effetti pregiudizievoli che la stessa potrebbe provocare sull´interessato.

Riepilogando, quindi, potrebbero essere utilizzati quali parametri per la valutazione del rischio:

- i controlli e le misure di sicurezza già in essere (quale, ad esempio, la crittografia);
- la tipologia dei dati oggetto della violazione (facendo particolare attenzione ai dati di traffico telefonico o telematico, nonché alle credenziali di autenticazione utilizzate dagli utenti);
- la tipologia della violazione verificatasi (ad esempio, accesso non autorizzato piuttosto che perdita o distruzione dei dati);
- l´identificabilità dei contraenti o delle altre persone coinvolte nella violazione (ad esempio, nel caso in cui la violazione abbia avuto ad oggetto più tipologie di dati relative alle medesime persone);
- l´attualità dei dati oggetto della violazione.

Nella valutazione di tali criteri indicativi, occorre che il fornitore tenga sempre conto dello specifico contesto nel quale si è verificato l´evento di violazione (vi sono, infatti, ambiti che presentano un maggiore grado di sensibilità, quali a titolo esemplificativo, quello sanitario o militare) e che nel dubbio venga preso in considerazione il caso peggiore, ossia quello nel quale la riservatezza o i dati personali dei contraenti o delle altre persone siano effettivamente pregiudicati dall´evento (ad esempio, la possibile esposizione a frodi nel caso di perdita di dati relativi alla carta di credito degli interessati).

8. Conseguenze per le ipotesi del mancato rispetto dei nuovi obblighi di sicurezza.

Per le ipotesi di violazione dei nuovi obblighi di sicurezza, il d.lg. n. 69/2012 ha introdotto nel Codice nuove e specifiche sanzioni amministrative (cfr. art. 162-ter) ed ha esteso quella penale prevista dall´art. 168 all´ipotesi di falsità nelle notificazioni al Garante ai sensi dell´art. 32-bis, commi 1 e 8.

L´art. 162-ter stabilisce che la omessa comunicazione della violazione di dati personali al Garante ex art. 32-bis, comma 1, nonché la ritardata comunicazione, ossia quella effettuata oltre i termini indicati al punto 5, è punita con la sanzione amministrativa del pagamento di una somma da venticinquemila euro a centocinquantamila euro; la omessa comunicazione della violazione di dati personali al contraente o ad altra persona ex 32-bis, comma 2, nonché la ritardata comunicazione, ossia quella effettuata oltre i termini indicati al punto 7, è punita con la sanzione amministrativa del pagamento di una somma da centocinquanta euro a mille euro per ciascun contraente o altra persona interessata.

In tale ipotesi, poi, il fornitore non può beneficiare del cumulo giuridico di cui all´art. 8 della legge n. 689/1981 e, tuttavia, la sanzione non può essere applicata in misura superiore al 5 per cento del volume d´affari realizzato dallo stesso nell´ultimo esercizio chiuso anteriormente alla notificazione della contestazione della violazione amministrativa, ferma restando la possibilità di aumento fino al quadruplo se le sanzioni risultino inefficaci in ragione delle condizioni economiche del contravventore, ai sensi dell´art. 164-bis, comma 4 (cfr. art. 162-ter, commi 2 e 3).

Ai sensi dell´art. 162-ter, comma 4, la violazione della disposizione concernente la tenuta di un aggiornato inventario delle

violazioni di dati personali, è punita con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro.

Le medesime sanzioni previste per i fornitori si applicano anche nei confronti dei soggetti ai quali sia stata affidata l´erogazione dei servizi, qualora tali soggetti abbiano omesso di comunicare senza ritardo al fornitore tutte le informazioni necessarie allo stesso per adempiere ai propri obblighi (art. 162-ter, comma 5).

L´art. 168 punisce, poi, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni il fornitore che dichiari o attesti falsamente notizie o circostanze, o produca atti o documenti falsi in occasione della comunicazione al Garante conseguente alla violazione di dati personali, nonché i soggetti, cui sia affidata l´erogazione del servizio, che effettuino false comunicazioni al fornitore.

TUTTO CIO´ PREMESSO IL GARANTE

ai sensi dell´art. 32-bis, comma 6, del Codice, stabilisce che i fornitori di servizi di comunicazione elettronica accessibili al pubblico come specificati in premessa sono tenuti a:

a. provvedere ad una prima, seppur sommaria, comunicazione al Garante della violazione dei dati personali subita entro il termine di 24 ore dall´avvenuta conoscenza della violazione, fornendo gli eventuali elementi ulteriori entro 3 giorni dalla stessa;

b. indicare nella comunicazione al Garante laddove la scoperta della violazione non sia stata contestuale al verificarsi dell´evento le ragioni che non hanno consentito l´immediata rilevazione dell´evento medesimo e le misure adottate o che si intende adottare affinché ciò non si ripeta;

c. fornire al Garante, sin dalla prima comunicazione dell´avvenuta violazione dei dati personali, almeno le seguenti informazioni:

1. i dati identificativi del fornitore;

2. una breve descrizione della violazione;

3. l´indicazione della data anche presunta della violazione e del momento della sua scoperta;

4. l´indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili;

5. l´indicazione della natura e della tipologia dei dati anche solo presumibilmente coinvolti;

6. una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

d. provvedere alla comunicazione ai contraenti o alle altre persone alle quali si riferiscono i dati personali oggetto della violazione entro il termine di 3 giorni dall´avvenuta conoscenza della violazione;

e. registrare nell´inventario il data breach che li ha coinvolti contestualmente alla comunicazione al Garante indicata al punto 5, avendo cura poi di inserire tempestivamente gli elementi che dovessero emergere successivamente, anche all´esito di ulteriori verifiche.

Si dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia ai fini della sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana a cura dell´Ufficio pubblicazione leggi e decreti.

Roma, 4 aprile 2013

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia

(*) Il modello va aperto, compilato e, dopo aver apposto la firma digitale, salvato come un file .pdf sul proprio computer. Infine, il modello va inviato al Garante **unicamente** tramite **posta PEC** all´indirizzo: dcrt@pec.gpdp.it.

Il modello è stato predisposto utilizzando lo standard di fatto PDF ed è leggibile attraverso un software gratuito e facilmente scaricabile in rete, oltre che nella disponibilità della generalità degli operatori ai quali è destinato il provvedimento del Garante. Per qualunque necessità il modulo può essere richiesto via PEC, anche in via precauzionale (prima che si verifichino eventuali violazioni) in modo da avere il modulo immediatamente disponibile per le eventuali notifiche al Garante. L´ufficio è disponibile per ogni ulteriore chiarimento, oltre che aperto ai suggerimenti che perverranno attraverso la consultazione pubblica.

VIOLAZIONE DI DATI PERSONALI

Allegato 1

Modello di comunicazione al Garante (fac simile - per le comunicazioni utilizzare ESCLUSIVAMENTE il MODELLO PDF appositamente predisposto)

1. Titolare che effettua la comunicazione:

    a. Denominazione o ragione sociale:

    b. Sede del titolare:

    c. Persona fisica addetta alla comunicazione:

    d. Funzione rivestita:

    e. Indirizzo email per eventuali comunicazioni:

    f. Recapito telefonico per eventuali comunicazioni:

2. Natura della comunicazione:

    a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.):

    b. Seguito di precedente comunicazione (inserire numero di riferimento):

        b.1. Inserimento ulteriori informazioni sulla precedente comunicazione:

        b.2. Ritiro precedente comunicazione (inserire le ragioni del ritiro):

3. Breve descrizione della violazione di dati personali:

4. Quando si è verificata la violazione di dati personali?

    a. Il …

    b. Tra il ….. e il …..

    c. In un tempo non ancora determinato

d. È possibile che sia ancora in corso

5. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

6. Modalità di esposizione al rischio:

a. tipo di violazione:

a.1. lettura (presumibilmente i dati non sono stati copiati)

a.2. copia (i dati sono ancora presenti sui sistemi del titolare)

a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

a.4. cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l´autore della violazione)

a.5. furto (i dati non sono più sui sistemi del titolare e li ha l´autore della violazione)

a.6. altro [specificare]

b. dispositivo oggetto della violazione:

b.1. computer

b.2. dispositivo mobile

b.3. documento cartaceo

b.4. file o parte di un file

b.5. strumento di backup

b.6. rete

b.7. altro [specificare

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

8. Quante persone sono state colpite dalla violazione di dati personali?

a. [numero esatto] persone

b. Circa [numero] persone

c. Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?

a. Dati anagrafici

b. Numeri di telefono (fisso o mobile)

c. Indirizzi di posta elettronica

d. Dati di accesso e di identificazione (user name, password, customer ID, altro)

e. Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

f. Altri dati personali (sesso, data di nascita/età, …), dati sensibili e giudiziari

g. Ancora sconosciuto

h. Altro [specificare]

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del titolare):

a. Basso/trascurabile

b. Medio

c. Alto

d. Molto alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione:

12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?

a. Sì, è stata comunicata il ….

b. No, perché [specificare]

13.Qual è il contenuto della comunicazione ai contraenti (o alle altre persone interessate)? [riportare il testo della notificazione]

14. Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?

15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?

a. No

b. Si

17. La comunicazione è stata effettuata alle competenti autorità di altri Paesi EU?

a. No

b. Si [specificare]