
WWW.CODICEORWELL.IT
TUTTI I VENERDI DALLE 8.00 ALLE 8.30
CODICE ORWELL
etica, diritti e doveri nella società digitale
[006] venerdi 5 Aprile 2024
L'EPOCA DEI DATA BREACH
a cura di
Santo Fabiano
e Marco La Diega

NORMATIVA

Articolo 4

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata** o **l'accesso ai dati personali trasmessi**, conservati o comunque trattati;

NORMATIVA

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

1. In caso di violazione dei dati personali, il **titolare** del trattamento **notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. **Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.**

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

NORMATIVA

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

3. La notifica di cui al paragrafo 1 deve almeno:

a) **descrivere la natura della violazione** dei **dati personali** compresi, ove possibile, **le categorie** e il **numero approssimativo di interessati** in questione nonché le categorie e il numero approssimativo di **registrazioni dei dati personali in questione**;

b) comunicare il **nome e i dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le **probabili conseguenze della violazione dei dati personali**;

d) descrivere **le misure adottate** o di cui si **propone l'adozione** da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

REGOLAMENTO UE 2016/679

Notifica di una violazione dei dati personali all'autorità di controllo

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Articolo 34

Notifica di una violazione dei dati personali all'autorità di controllo

REGOLAMENTO UE 2016/679

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

GARANTE

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ACCEDI AL SERVIZIO TELEMATICO DEDICATO AL DATA BREACH

Notifica di una violazione dei dati personali (data breach)

art. 33 del Regolamento (UE) 2016/679 - art. 26 del D.Lgs. 51/2018

COMPILAZIONE DELLA NOTIFICA

Disponibile a breve

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

PAGINA INFORMATIVA - VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

AUTO VALUTAZIONE PER LA NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

FAC-SIMILE DEL MODELLO

ISTRUZIONI

www.codiceorwell.it

GARANTE

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?*

Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

na violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Si verifica:

una **violazione della riservatezza** in caso di divulgazione dei dati o accesso agli stessi non autorizzati o accidentali;

una **violazione dell'integrità** in caso di modifica non autorizzata o accidentale dei dati;

una **violazione della disponibilità** in caso di perdita o distruzione non autorizzate o accidentali di dati.

santofabiano.it

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

santofabiano.it

GARANTE

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere **accompagnate dai motivi del ritardo.**

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

santofabiano.it

COME INVIARE LA NOTIFICA AL GARANTE?

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (VEDI: Provvedimento del 27 maggio 2021).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

santofabiano.it

LE AZIONI DEL GARANTE

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

santofabiano.it

www.garanteprivacy.it

URP e servizi utili

Nello sportello dei servizi è possibile trovare informazioni riguardanti

Modulistica e servizi online

Motore di ricerca FAQ

Reclami e Segnalazioni

CONTATTA L'URP

L'URP (Ufficio Relazioni con il Pubblico) risponde a quesiti e offre informazioni su disposizioni in materia di trattamento e protezione dei dati personali, modalità di tutela (reclami, segnalazioni), richieste di documentazione e materiale informativo.

- ACCEDI AL SERVIZIO TELEMATICO DEDICATO ALLA SEGNALAZIONE DI COMUNICAZIONI INDESIDERATE (TELEMARKETING)
- ACCEDI AL SERVIZIO TELEMATICO DEDICATO ALLA SEGNALAZIONE PER PREVENIRE IL FENOMENO REVENGE PORN
- ACCEDI AL SERVIZIO TELEMATICO DEDICATO AL DATA BREACH
- ACCEDI AL SERVIZIO DI COMUNICAZIONE DEI DATI DI CONTATTO DELL'RPD

Notifica di una violazione dei dati personali (data breach)

art. 33 del Regolamento (UE) 2016/679 - art. 26 del D.Lgs. 51/2018

Auto valutazione per la notifica di una violazione dei dati personali (data breach)

Compilazione della notifica

Istruzioni

Informativa sul trattamento dei dati personali

Pagina informativa - Violazione dei dati personali (data breach)

Fac-simile del modello

F) Informazioni sulla violazione

1. Momento in cui è avvenuta la violazione

- a) Il ___ /___ /_____
- b) Dal ___/___ /_____ (la violazione è ancora in corso)
- c) Dal ___/___ /_____ al ___ /___ /_____
- d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

santofabiano.it

Il modello di notifica di una violazione dei dati personali

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- a) Rilevazione da parte del titolare[1]
- b) Comunicazione da parte del responsabile del trattamento
- c) Segnalazione da parte di un interessato
- d) Segnalazione da parte di un soggetto esterno
- e) Notizie stampa
- f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data ..... **Ora** .....

4. *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

santofabiano.it

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2]
[ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna
[ ] b) Azione accidentale interna
[ ] c) Azione intenzionale esterna
[ ] d) Azione accidentale esterna
[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

santofabiano.it

8. Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione

9. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti

santofabiano.it

10. *Categorie di interessati coinvolti nella violazione*

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

11. *Numero (anche approssimativo) di interessati coinvolti nella violazione*

- a) N. ..... interessati
- b) Circa n. ..... interessati
- c) Non determinabile
- d) Non ancora determinato

GARANTE
santofabiano.it

Il modello di notifica di una violazione dei dati personali

12. *Categorie di dati personali oggetto di violazione*

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici
[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

santofabiano.it

Il modello di notifica di una violazione dei dati personali

13. Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione

- a) N. ……..
- b) Circa n. ……..
- c) Non determinabile
- d) Non ancora determinato

14. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati

15. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

santofabiano.it

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

[ ] a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
[ ] d) Altro

[ ] e) In corso di valutazione[4]

santofabiano.it

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi
[ ] c) Altro

[ ] d) In corso di valutazione[4]

santofabiano.it

2. *Potenziale impatto per gli interessati*

[ ] a) Perdita del controllo dei dati personali
[ ] b) Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità
[ ] e) Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione
[ ] h) Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale
[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

santofabiano.it

H) Misure adottate a seguito della violazione

1. ***Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati***

2. ***Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future***

GARANTE

santofabiano.it

Il modello di notifica di una violazione dei dati personali

1. *Il titolare del trattamento ritiene[1] che:*

- a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

santofabiano.it

Nel caso in cui la violazione riguardi un servizio affidato all’esterno

È necessario acquisire dal “responsabile del trattamento” (società o professionista a cui è affidato il servizio) tutte le informazioni utili per la compilazione di modello di notifica della violazione al Garante

santofabiano.it

Fac simile richiesta informazioni al “responsabile” esterno

Codesta società, in qualità di Responsabile del trattamento, a seguito dell’affidamento dei servizi di….. avvenuto con ….., in data xxx ha comunicato per email la possibile violazione del trattamento di dati personali riguardanti gli stessi servizi affidati, in conseguenza della quale, questo ente non risulta in condizione di poterne fruire.

Si precisa, preliminarmente, che sorprende di rilevare che sul sito di codesta società appare una comunicazione dell’xxx che annuncia l’avvenuta violazione, mentre la notizia è stata trasmessa a questo ente, quale titolare del trattamento, soltanto il xxx. Né, in quest’ultima circostanza sono state forniti informazioni utili per comprendere le dimensioni dell’accaduto, le eventuali conseguenze, le misure adottate e le iniziative intraprese, anche con riferimento alle segnalazioni alle autorità competenti.

Questo ente, una volta acquisita la comunicazione ha provveduto a inoltrare al Garante la dovuta segnalazione che tuttavia risulta carente proprio a causa della mancata comunicazione delle informazioni richiesta da parte di codesta società.

Pertanto si riporta di seguito una serie di informazioni che si richiedono allo scopo di potere avere cognizione dell’accaduto e dei rischi connessi, oltre che per fornire al Garante le informazioni richieste dal modello di data breach.

Allo scopo di facilitare la comprensione di quanto richiesto sono riportati, per ogni informazione, i riferimenti relativi al modello predisposto dal Garante.

Informazioni richieste:

F.5: natura della violazione

F.6: causa della violazione

F.7: descrizione della violazione

F.8: Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione

F.9: Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti

H.1 Misure tecniche e organizzative adottate per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati

H.2 Misure tecniche e organizzative adottate per prevenire simili violazioni future

M.1 La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative1?

M.2 È stata effettuata la segnalazione all’autorità giudiziaria o di polizia?

N.1 La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all’interno dello Spazio Economico Europeo?

Si rappresenta l’urgenza di avere le informazioni richieste allo scopo di definire la procedura di data breach.

santofabiano.it

Data breach: il Garante sanziona UniCredit per 2,8 milioni di euro*
Multa di 800mila euro anche alla società incaricata di effettuare i test di sicurezza

*Il provvedimento è stato impugnato innanzi al Tribunale di Milano, che ha disposto la sospensione dell'efficacia della sanzione accessoria della pubblicazione del provvedimento sul sito web del Garante con ordinanza n. 1927 del 28 marzo 2024 (RG n. 10477/202)

Le banche devono adottare tutte le necessarie misure tecnico-organizzative e di sicurezza per evitare che i dati dei propri clienti possano essere sottratti illecitamente. Lo ha affermato il Garante per la privacy nel sanzionare UniCredit banca per una violazione di dati personali (data breach) avvenuta nel 2018, che ha coinvolto migliaia di clienti ed ex clienti.

Dalle verifiche effettuate dall'Autorità - a seguito della ricezione della notifica di data breach da parte della banca - è emerso che la violazione era avvenuta a causa di un attacco informatico massivo, perpetrato da cybercriminali, al portale di mobile banking. L'attacco aveva causato l'acquisizione illecita del nome, cognome, codice fiscale e codice identificativo di circa 778mila clienti ed ex clienti e, per oltre 6.800 dei clienti "attaccati", aveva comportato anche l'individuazione del PIN di accesso al portale. I dati erano resi disponibili nella risposta HTTP fornita dai sistemi della banca al browser di chiunque provasse ad accedere, anche senza riuscirvi, al portale di mobile banking.

Nel corso della complessa attività istruttoria, il Garante ha rilevato diverse violazioni della normativa privacy. In particolare, l'Autorità ha accertato che la banca non aveva adottato misure tecniche e di sicurezza in grado di contrastare efficacemente eventuali attacchi informatici e di impedire ai propri clienti di utilizzare PIN deboli (come ad es. quelli composti da sequenze di numeri o coincidenti con la data di nascita). Nel definire l'importo della sanzione a 2 milioni e 800 mila euro, il Garante ha considerato l'elevato numero dei soggetti coinvolti dalla violazione dei dati personali, la gravità della stessa e la capacità economica della banca. Sono invece state considerate attenuanti la tempestiva adozione di misure correttive, le iniziative di informazione e supporto poste in essere nei confronti della clientela e la circostanza che la violazione non ha riguardato i dati bancari.

Con l'adozione di un secondo provvedimento l'Autorità è intervenuta anche nei confronti di NTT Data Italia, sanzionando la società con una multa di 800mila euro. Dalle verifiche effettuate dal Garante, in particolare è emerso che NTT Data Italia aveva comunicato ad UniCredit l'avvenuta violazione dei dati personali dei propri clienti oltre il termine previsto dal Regolamento e solo dopo che la banca ne era venuta a conoscenza tramite i propri sistemi di monitoraggio interno.

Inoltre, NTT Data Italia aveva affidato l'esecuzione delle attività di vulnerability assessment e penetration testing in subappalto ad un'altra società, senza l'autorizzazione preventiva alla banca in qualità di titolare del trattamento, che invece aveva espressamente vietato l'affidamento a terze parti di tali attività.

App per diabetici: il Garante Privacy multa una società di dispositivi medici
Aveva inviato in chiaro e-mail a centinaia di pazienti diabetici

Il Garante privacy ha comminato due sanzioni per complessivi 300mila euro a una nota società che produce dispositivi medici per il monitoraggio, la prevenzione e il trattamento di diverse patologie.

La prima, di 250mila euro, è stata applicata alla società per aver inviato alcune e-mail con gli indirizzi, in chiaro, di centinaia di destinatari, malati di diabete, che utilizzavano una sua app per la misurazione dei livelli di glucosio.

L'altra di 50mila euro, per non aver fornito un'informativa completa ai pazienti, fruitori dei servizi di healthcare.

Nel corso dell'istruttoria è emerso che, nell'inviare le e-mail aventi ad oggetto un aggiornamento dell'applicazione, quindi una comunicazione di servizio, l'inserimento degli indirizzi email nel campo "copia per conoscenza" anziché in "copia nascosta", aveva consentito a tutti i destinatari di vedere gli indirizzi contenuti nella mailing list, con la conseguente comunicazione, da parte della società, a terzi non autorizzati, di dati personali estremamente delicati, come quelli relativi alla salute.

L'incidente metteva anche in evidenza la mancata adozione da parte della società di misure tecniche e organizzative adeguate a ridurre il rischio di un data breach.

Dagli accertamenti del Garante per verificare la conformità dei trattamenti effettuati mediante i servizi offerti all'utenza, sono emerse inoltre altre violazioni che sono state considerate separatamente ai fini della quantificazione della sanzione amministrativa. In particolare, nell'informativa, non era indicata la base giuridica in virtù della quale veniva effettuata la comunicazione di dati personali dei pazienti che intendevano collegare il proprio account personale con quello del professionista sanitario, in qualità di titolare del trattamento, in violazione del principio di correttezza e trasparenza.

Data breach

Che cos'è

Con il termine **data breach** si intende un incidente di sicurezza in cui dati sensibili, riservati, protetti vengono consultati, copiati, trasmessi, rubati o utilizzati da soggetti non autorizzati. Solitamente il data breach si realizza attraverso una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezza (come ad esempio il web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- **perdita accidentale**: data breach causato ad esempio da smarrimento di una chiavetta USB con contenuti riservati;
- **furto**: data breach causato ad esempio da furto di un notebook con all'interno dati confidenziali/riservati;
- **infedeltà aziendale**: data breach causato ad esempio da un dipendente/persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia da distribuire in ambiente pubblico;
- **accesso abusivo**: data breach causato ad esempio da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

Secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, **entro 72 ore**, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

santofabiano.it

Agenzia: CSIRT Italia: ITA

Agenzia per la cybersicurezza nazionale

Segnala un incidente informatico

Agenzia PNRR Cloud Lavora con noi Amministrazione trasparente

santofabiano.it

CSIRT Italia

Il Computer Security Incident Response Team di ACN si occupa principalmente delle attività di natura reattiva; costituisce l'interfaccia con i soggetti esterni ai quali, oltre a fornire supporto in caso di incidente informatico, indirizza i prodotti di allertamento preventivo sulle minacce e relative attività di mitigazione.

Scopri di più

santofabiano.it

DECRETO LEGISLATIVO 18 maggio 2018, n. 51

Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

santofabiano.it

Articolo 25

D.lgs. 18 maggio 2018, n. 51
Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio

Sicurezza del trattamento

1. Il titolare del trattamento e il responsabile del trattamento, tenuto conto delle cognizioni tecniche disponibili, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del grado di rischio per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati.

Articolo 25

D.lgs. 18 maggio 2018, n. 51
Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio

Sicurezza del trattamento

2. Per il trattamento automatizzato il titolare o il responsabile del trattamento, previa valutazione dei rischi, adottano misure volte a:

a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);

c) impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);

e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f) garantire la possibilità di individuare i soggetti ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

l) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Articolo 25

D.lgs. 18 maggio 2018, n. 51
Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio

Sicurezza del trattamento

1. Salvo quanto previsto dall'articolo 37, comma 6, in caso di violazione di dati personali, il titolare del trattamento notifica la violazione al Garante con le modalità di cui all'articolo 33 del regolamento UE.

2. Se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni previste dal citato articolo 33 del regolamento UE sono comunicate, senza ingiustificato ritardo, al titolare del trattamento di tale Stato membro.

GPDP
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione Annuale 2022