



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## Violazioni di dati personali (data breach): gli adempimenti previsti - L'infografica del Garante privacy

### Violazioni di dati personali (*data breach*): gli adempimenti previsti - L'infografica del Garante privacy

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Per questa ragione, anche sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali (*data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

I casi e gli adempimenti previsti dai provvedimenti del Garante [doc. web nn. [2388260](#), [3556992](#), [4084632](#) e [4129029](#)] sono riassunti in una [infografica](#) che offre un prospetto sintetico sulla materia.

**Violazioni di dati personali (*data breach*)**  
Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che fissano per amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati. La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.

**SOCIETÀ TELEFONICHE E INTERNET PROVIDER**  
Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- L'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tic e isp devono:
  - entro 24 ore dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione;
  - entro 3 giorni dalla scoperta, informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti non è dovuta se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un inventario costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

**BIOMETRIA**  
Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- Entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

**DOSSIER SANITARIO ELETTRONICO**  
Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- Entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

**AMMINISTRAZIONI PUBBLICHE**  
Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- Entro 48 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Per approfondimenti, consultare i provvedimenti pubblicati sul sito: [www.garanteprivacy.it](http://www.garanteprivacy.it)

### I PROVVEDIMENTI CITATI NELL'INFOGRAFICA

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

- [Provvedimento generale prescrittivo in tema di biometria 12 novembre 2014](#)

- [Linee guida in materia di Dossier sanitario 4 giugno 2015](#)

- [Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche 2 luglio 2015](#)