



➡ **Perché è necessario adeguare il condominio alla normativa sulla privacy?**

Nel febbraio del 2006 il Garante della Privacy si è trovato di fronte ad un quesito posto dalle associazioni di categoria degli amministratori di condominio. Il quesito verteva sulla necessità di chiarire se il condominio rientrasse nell'applicazione della normativa sulla privacy e in che modo dovesse essere poi eventualmente applicata. Dal maggio 2006 il Garante ha iniziato a dare una serie di informazioni e chiarimenti utili. Infatti la prima cosa da comprendere, per capire se il condominio rientrasse nell'applicabilità della normativa privacy, era chiarire se il condominio fosse ritenuto Titolare del trattamento dati e se lo fosse l'Amministratore. Nel giugno del 2006 con un comunicato stampa il Garante dice "Il condominio, in quanto titolare del trattamento, può trattare solo **informazioni personali pertinenti e necessarie** per la gestione e l'amministrazione delle parti comuni. Le informazioni possono riguardare sia tutto il condominio (dati relativi a consumi collettivi), sia i singoli partecipanti (dati anagrafici, indirizzi, quote millesimali). [...] Per prevenire illecite comunicazioni e diffusioni di dati personali l'amministratore deve adottare **idonee misure di sicurezza** previste dal Codice della Privacy." Con queste dichiarazioni il Garante determina che il Titolare dei dati è il condominio, quindi rientra nell'applicabilità della normativa e il compito dell'Amministratore è quello di eseguire quanto stabilito dal testo di legge che identifica nelle misure di sicurezza richieste i seguenti elementi:

Allegato tecnico: Trattamenti senza l'ausilio di strumenti elettronici Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

- Agli incaricati (**amministratore, dipendenti/collaboratori studio, consulenti esterni quali commercialista, consulente del lavoro, avvocato ...**) sono impartite istruzioni scritte (**lettere di nomina**) finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali (**elenco banche dati**).
- Nell'ambito **dell'aggiornamento periodico con cadenza almeno annuale** dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.



- L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Ora andiamo a vedere che tipo di dati sensibili tratta il condominio estrapolando le informazioni dal Provvedimento del maggio 2006

“[...] Possono altresì formare oggetto di trattamento nell'ambito delle menzionate finalità di amministrazione del condominio, dati personali di natura sensibile o dati giudiziari, nella misura indispensabile al perseguimento delle medesime finalità.

Tale ipotesi può ricorrere, ad esempio, in relazione al trattamento di dati di natura sensibile e giudiziaria del personale alle dipendenze del condominio in ordine al quale, salvo l'obbligo di rendere l'informativa ai sensi dell'art. 13 del Codice, trovano applicazione lo speciale presupposto di cui all'art. 26, comma 4, lett. d), del Codice (obblighi del datore di lavoro) e le autorizzazioni generali del Garante nn. 1 e 7 del 2005 (relative al trattamento dei dati sensibili nei rapporti di lavoro e ai dati giudiziari).

Ulteriori ipotesi di trattamento di dati sensibili nell'ambito dell'amministrazione condominiale possono comunque configurarsi: si pensi al trattamento di dati sanitari effettuato in relazione a danni alle persone, anche diverse dai condomini, e ai trattamenti di dati sanitari di uno o più partecipanti connessi all'adozione di una delibera assembleare avente ad oggetto l'abbattimento delle c.d. "barriere architettoniche".

Sempre nel sopracitato Provvedimento si stabilisce che

“Solo in presenza del consenso dell'interessato (**informativa firmata**)(salva l'eventuale pubblicità già attribuita a tali informazioni grazie alla loro indicazione in elenchi pubblici), invece, possono essere trattate, in quanto non eccedenti rispetto alla finalità di amministrazione della cosa comune, le informazioni relative alle utenze telefoniche intestate ai singoli partecipanti: il loro utilizzo, infatti, può agevolare, specie in relazione a casi particolari di necessità ed urgenza (ad esempio al fine di prevenire o limitare eventuali danni a parti individuali o comuni dell'immobile), i contatti tra i partecipanti come pure lo svolgimento delle incombenze rimesse all'amministratore del condominio (cfr. Provv. **19 maggio 2000**, in Boll. n. 13/2000, p. 7, **doc. web n. 42268**).” La necessità del consenso scritto viene poi ripreso anche nel Vademecum del palazzo pubblicato nel 2010 dal garante della Privacy.

Responsabile Centro Studi

Monica Dott.ssa Del Toro



Codice in materia di protezione dei dati personali

B. Disciplinare tecnico in materia di misure minime di sicurezza

(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. [soppresso] ⁽¹⁾

- 19.1. [soppresso]⁽¹⁾
- 19.2. [soppresso]⁽¹⁾
- 19.3. [soppresso]⁽¹⁾
- 19.4. [soppresso]⁽¹⁾
- 19.5. [soppresso]⁽¹⁾
- 19.6. [soppresso]⁽¹⁾
- 19.7. [soppresso]⁽¹⁾
- 19.8. [soppresso]⁽¹⁾



Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. [soppresso] ⁽¹⁾

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

(1) Paragrafi soppressi 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.

Per completezza, si riporta di seguito il testo dei paragrafi soppressi.

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- 19.1. l'elenco dei trattamenti di dati personali;
- 19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- 19.3. l'analisi dei rischi che incombono sui dati;
- 19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- 19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
- 19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- 19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- 19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.