# GDPR Amministrazione (Responsabilità)

*Mini guida sulla privacy*

## Sommario

*Introduzione*

Con l'entrata in vigore del Regolamento Europeo 2016/679 (GDPR) l'Europa ha preferito optare per l'applicazione del

***principio di accountability***

cioè il principio per il quale il titolare del trattamento dei dati personali compie le sue scelte di gestione e di sicurezza e poi ne risponde per **responsabilità** laddove qualcosa non vada bene. Per sintetizzare, il concetto si potrebbe riassumere così:

> ***Salvo circostanze particolari non ti impongo oneri specifici nella gestione dei dati personali. Fai tu, ma se si creano problemi passerai dei brutti momenti.***

In Italia siamo abituati a ragionare in altro modo. Dimmi che devo fare e io mi adeguo. **La prima importante rivoluzione di questo GDPR è dunque culturale, di approccio.** Una **responsabilizzazione del titolare** al posto del controllo sul compito svolto.

**Per essere in regola, quindi, bisogna capire la nuova privacy** – il che non è scontato né automatico. Capire la privacy, perché sulla base di quelli che sono i trattamenti da effettuare si dovrà valutare quali sono le procedure da applicare.

A prescindere da tutto, è comunque necessario avere chiara la situazione

- della propria attività;
- della propria organizzazione interna;
- di quali tipologie di dati tratto, di quali tipologie di trattamenti effettuo;
- di quali rischi corrono i dati trattati con certe modalità, se effettuo trasferimenti di dati …

Per la professione di **amministratore di condominio**, è utile valutare che impatto abbia avuto l'entrata in vigore del **GDPR e cosa debba fare il professionista per essere in regola**.

È importante evidenziare che la maggior parte degli oneri posti a carico del titolare del trattamento riguarda le società con oltre 250 dipendenti o con caratteristiche specifiche, il che esclude che tali regole siano obbligatorie per la categoria degli amministratori di condominio.

Un esempio per tutti. Si è sentito parlare moltissimo della figura del DPO (Data Protection Officer) il responsabile della protezione dei dati. **La nomina di tale figura, nel caso dell'amministratore di condominio, non è obbligatoria**. Di certo, tuttavia, la nomina di un DPO è utilissima anche nel caso in cui non sia obbligatoria e personalmente consiglio di effettuarla, salvo realtà molto ridotte.

## Condominio on the Net

L'adeguamento - **allegato 1** - (Interfacce, accessi, database, canali di comunicazione, ...) proposto con l'entrata in vigore del GDPR è stato portato a termine come indicato nell'**allegato 2**. Il resto della guida suggerisce procedure interne all'Amministrazione che devono essere portate a termine.

## Cosa deve fare l'amministratore di condominio?

- In primo luogo **fare un check sulla struttura del suo ufficio.** La cosa migliore è quella di creare un organigramma, specificando chiaramente chi fa cosa su quali dati personali. Così

facendo si potranno avere chiari i ruoli e le responsabilità e predisporre pertanto quei documenti che sono necessari per un lecito trattamento dei dati. Facciamo il caso di uno studio di amministrazione con due amministratori in società di persone, si potrà configurare il caso di contitolarità del trattamento, oggi regolamentato dall'art.26 del GDPR. Nel caso di uno o più dipendenti si potranno configurare una serie di "incaricati del trattamento" che per trattare lecitamente i dati dei condomini devono ricevere dall'amministratore una specifica lettera di incarico che li autorizzi a compiere determinate operazioni sui dati personali e solo quelle. Un organigramma aggiornato e strutturato in questo modo consente anche di redigere una corretta informativa da fornire a tutti.

- **L'informativa** deve essere cambiata rispetto a quella che avevamo prima dell'ingresso del GDPR. Oggi sono stati introdotti nuovi diritti degli interessati, sono state inserite nuove informazioni che devono essere fornite ed anche le tempistiche sono un po' modificate. Ovviamente quello che si scrive nell'informativa deve essere vero, per cui è necessario che realmente il titolare sia in grado di dare pronto riscontro all'interessato che avanzi una legittima richiesta o eserciti un suo diritto. Per cui è utile predisporre una serie di procedure, magari **corredate di idonea modulistica**, che consenta un riscontro efficace. Una di queste è la predisposizione e compilazione di un registro dei trattamenti previsto dall'art.30 del GDPR – ma obbligatorio solo nei casi ivi previsti (più di 250 dipendenti, trattamento di dati particolari art.9 GDPR, trattamento di dati giudiziari…).
- Elemento chiave è la **gestione della sicurezza**. Le misure da applicare per proteggere un trattamento dati personali cambiano a seconda di quali dati si trattino ed in che modalità si trattino. Un numero di telefono sulla rubrica di un cellulare o su un'agenda cartacea deve essere gestito in diverso modo e protetto in diverso modo. Anche in questo caso una corretta analisi della propria struttura potrà aiutare l'amministratore a capire quale sia il complesso di misure (fisiche, logiche ed organizzative) utili per raggiungere lo scopo.
- In questo contesto si colloca anche la **valutazione di impatto sulla protezione dei dati personali** che bisogna effettuare nei casi previsti dall'art.35 GDPR e che è comunque fortemente consigliata ogni qual volta il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche. L'analisi dei rischi è una risorsa importante per ragionare su quello che si sta facendo e su come lo si sta facendo.
- **L'amministratore in genere non deve chiedere il consenso ai condomini per trattare i loro dati personali**, in quanto la base giuridica del trattamento è l'esecuzione del mandato conferitogli. Tuttavia ci possono essere situazioni particolari in cui l'amministratore debba trattare dati particolari, sanitari o di giustizia, ed in quel caso è sempre utile avere un consenso scritto che autorizzi il trattamento e, se necessario, autorizzi anche la comunicazione dei dati ad altri.

## Sintetizzando in pratica, verso i condomini l'amministratore deve:

- **Redigere una informativa aggiornata e portarla a conoscenza dei condomini** con i mezzi più idonei (sito web, comunicazione ad personam, con conferma di ricezione o in modalità telematica, bacheca condominiale, ...);
- deve **acquisire il consenso laddove** il trattamento non sia diretto svolgimento del mandato assembleare o vi siano dati rilevanti da tutelare;
- **deve aver curato la sua organizzazione interna** in modo che il lavoro sia svolto nel rigido rispetto dei diritti degli interessati, con accorgimenti tecnici e standardizzazione di procedure.

Sulla base di quanto detto è totalmente inutile fare compilare documenti e scartoffie da un consulente.
Che senso ha avere i documenti nel cassetto, se poi il processo secondo cui si trattano i dati personali è del tutto inaffidabile?
L'obiettivo è di erigere un sistema da integrare con un sistema di gestione della Privacy senza lasciare nulla al caso, in modo da non rendere possibile un tentativo di furto o una fuga di dati personali.

## Il GDPR non è solo

- un adeguamento burocratico *("Ho fatto le nomine a tutti, sono a posto …")*
- un adeguamento tecnologico *("Ho comprato il firewall, ho comprato un software per fare il registro dei trattamenti che mi risolve tutti i problemi …")*
- la paura delle sanzioni *("potresti prendere una multa fino a 20 milioni di euro, se non ti adegui subito …")*
- l'ennesimo costo aggiuntivo che grava sulle aziende *("Con 900 euro ho fatto tutto …")*

## E allora, cos'è questo GDPR?

deve essere prima di tutto una presa di

## RESPONSABILITÀ, CONSAPEVOLEZZA E FORMAZIONE

I comportamenti delle persone sono la prima causa di incidenti informatici, proprio perché manca la consapevolezza del valore dei dati.

> ***(Lascereste 100 euro sulla scrivania prima di andare a pranzo? E allora perché lasciate il pc accesso senza neanche una password sul salvaschermo?)***

Il GDPR è un insieme di regole condivise per proteggere le informazioni personali. Uno degli adempimenti più importanti è infatti proprio l'informativa, il patto tra il cliente che affida i suoi dati e l'azienda che deve gestirli.

> ***(Dareste 100 euro al primo che passa senza neanche chiedere cosa intende farne? Ecco questa è l'informativa, cioè l'insieme di informazioni che viene dato all'interessato per aumentare la sua consapevolezza e fiducia.)***

**La principale misura di sicurezza è la formazione.**
Non confondere la sicurezza informatica con la sicurezza delle informazioni, non a caso, la misura di sicurezza più importante è proprio la formazione, che serve per aumentare la consapevolezza e la conoscenza delle minacce a cui si può essere sottoposti, non c'è malware che tenga se l'utente è sprovveduto.
Il GDPR si fonda sui principi di **Accountability, Privacy by design e Privacy by default.**
Per conoscere le regole del nuovo regolamento privacy, e quindi esserne pienamente responsabile e consapevole, è necessario che l'amministratore e i dipendenti abbiano una formazione adeguata per comprendere appieno la portata di questa legge. Non c'è nulla di difficile, ma certamente è necessario capire i punti chiave, anche solo per evitare il rischio di incorrere in pesanti sanzioni.

Per prima cosa occorre definire una serie di figure nell'azienda anche se è piccola. **Uno studio di amministrazioni condominiali con dei dipendenti dovrà avere una struttura organizzativa adeguata:**

### TITOLARE DEL TRATTAMENTO DEI DATI

Per quanto riguarda le amministrazioni condominiali il **Titolare del trattamento** dei dati è l'**amministratore del condominio** stesso, colui che di fatto ha la responsabilità legale dell'azienda.

### RESPONSABILE DEL TRATTAMENTO DEI DATI

A meno che non si tratti di un'organizzazione complessa, non è necessario nominare un ulteriore **Responsabile per il trattamento** dei dati, perché sarà lo stesso **amministratore**.

### INCARICATI DEL TRATTAMENTO DEI DATI

Gli incaricati, siano essi dipendenti interni oppure consulenti esterni, sono quelle persone che operativamente trattano i dati dell'azienda e dei condomini. Ad esempio:

- Dati relativi l'assemblea
- Dati relativi la bacheca condominiale
- La gestione trasparente del condominio
- La videosorveglianza
- Il condominio digitale
- Diritto di accesso ai propri dati e altri diritti
- Consulente del lavoro: dati dei dipendenti
- Commercialista: dati di clienti e fornitori
- Consulente informatico: tutti i dati informatici

**Tutti gli incaricati dovranno firmare specifiche lettere di consenso**.

## RUOLI DELL'AMMINISTRATORE IN AMBITO PRIVACY

L'amministratore può essere nominato dall'assemblea quale "**Responsabile del trattamento**" dei dati personali con lo scopo di ottemperare a tutte le esigenze di trasparenza compatibili con quelle di riservatezza.
I dati personali che si possono trattare in qualità di AMMINISTRATORE DI CONDOMINIO sono unicamente quelli che **non eccedono le finalità** di gestione e amministrazione degli stabili (dati anagrafici, indirizzo, ecc.).

Possono inoltre essere utilizzati:

- i numeri di telefono fisso, cellulare o indirizzo di posta elettronica se già indicati in elenchi pubblici o forniti direttamente dal condomino, fermo restando il fatto che il loro utilizzo deve essere ponderato secondo le regole del buon senso;
- i dati sensibili (stato di salute) o giudiziari, indispensabili per l'amministrazione del condominio. Se sono trattatati dati che riguardano terze persone, queste ultime devono essere informate sulle finalità e le modalità del trattamento stesso.

L'amministratore ha, infine, l'obbligo di:

- Conservare la documentazione relativa ai condomini (cartacea o telematica);
- Predisporre misure di sicurezza per proteggere i dati, specie se sensibili;
- Comunicare ai condomini i propri dati anagrafici e professionali (codice fiscale e, se si tratta di società, la sede legale e la denominazione). Tali dati devono essere portati a conoscenza dei condomini mediante affissione nel condominio.

**In sintesi, l'amministratore può:**

- acquisire le informazioni che consentono di identificare e contattare i singoli partecipanti al condominio (siano essi proprietari, usufruttuari, conduttori o comodatari) chiedendo le generalità comprensive di codice fiscale, residenza o domicilio;
- chiedere i dati catastali: la sezione urbana, il foglio, la particella, il subalterno e il comune. Non può invece chiedere, perché risulterebbe eccedente, copia della documentazione come ad esempio l'atto di compravendita in cui sono riportati i dati;
- raccogliere dati ai fini della valutazione delle "condizioni di sicurezza" che riguardano le parti in comune dell'edificio e non le singole unità immobiliari.

## GESTIONE DELL'ASSEMBLEA

L'assemblea è un altro momento nel quale una serie di dati e di informazioni possono essere rese disponibili anche a terzi e quindi occorre prendere qualche precauzione. Infatti qualora all'assemblea partecipino **soggetti terzi** come tecnici e consulenti chiamati per discutere su particolari questioni, come l'approvazione di specifici lavori che richiedono una consulenza, questi ultimi **possono rimanere solo per trattare quel determinato punto** per cui è richiesta la loro presenza dall'ordine del giorno. Sarebbe inoltre buona cosa far firmare a questi esterni un impegno di riservatezza e di non utilizzo delle informazioni di cui sono venuti a conoscenza durante l'assemblea. L'assemblea può essere videoregistrata purché le registrazioni siano opportunamente custodite dall'amministratore del condominio e con il preventivo consenso informato di tutti i partecipanti. Anche qui occorre far firmare il consenso a tutti i partecipanti.

## BACHECA CONDOMINIALE

La bacheca condominiale è un altro di quegli strumenti a disposizione dell'amministratore per divulgare informazioni inerenti la gestione dell'immobile.
Anche in questo caso l'amministratore deve fare un po' di attenzione a cosa viene inserito in ogni specifica bacheca.
Il Garante Privacy si è anche pronunciato in merito e ha previsto che nella bacheca condominiale:

- non possono essere inserite comunicazioni concernenti i dati personali dei singoli condomini;
- non possono essere affissi i verbali di assemblea per i condomini assenti;
- non possono esservi contenute comunicazioni circa la morosità (che consiste nel ritardo nel pagamento delle spese condominiali) di uno o più condomini (argomento che può essere oggetto di discussione solo in assemblea).

## GESTIONE TRASPARENTE DEL CONDOMINIO

Ogni condomino, in tema di trasparenza, ha diritto a:

- conoscere tutte le informazioni e i dati raccolti che lo riguardano;
- conoscere le spese e gli inadempimenti degli altri condomini, ad esclusione di quelle al di fuori dell'ambito condominiale per le quali vi è il divieto di diffusione (questo dato lo può conoscere solo il singolo condomino in maniera privata e tale dato non può essere divulgato in forma collettiva).
- farsi aggiornare, rettificare o integrare i dati che lo riguardano o chiedere la trasformazione o la cancellazione se trattati contro la legge. In caso di cessazione del rapporto tra il condomino e l'amministratore vale il principio del **DIRITTO ALL'OBLIO**, sancito dal nuovo Regolamento 679/2016, ovvero **la cancellazione e distruzione** sia cartacea che digitale di tutte le informazioni personali che riguardano il condomino stesso.

L'amministratore ha l'obbligo di:

- comunicare ai creditori che ne facciano richiesta, i dati dei condomini morosi;
- aprire un conto corrente postale o bancario intestato al condominio per farvi transitare le somme percepite a qualsiasi titolo per conto del condominio stesso.
- ogni condomino ha diritto di prendere visione ed estrarre copia del rendiconto periodico; infatti, il Garante Privacy ha specificato che ad ogni condomino è consentito accedere alla documentazione e agli estratti bancari e/o postali del Condominio, tramite l'amministratore, e di ottenere copia senza alcuna limitazione (anche se contengono dati personali riferiti a terzi).

## VIDEOSORVEGLIANZA

Anche per quanto concerne il discorso della videosorveglianza e dell'installazione di videocamere di sorveglianza, che è un argomento piuttosto complicato, occorre che l'amministratore del condominio faccia alcune attente valutazioni preventive.
Soprattutto occorre distinguere due concetti fondamentali e le relative FINALITÀ:

- **La salvaguardia delle singole proprietà immobiliari**: si ha nel caso in cui il singolo condomino installi tali apparecchi per fini esclusivamente personali e nell'ambito del proprio appartamento. Non si applicano, in tal caso, le norme sulla privacy, a meno che tali installazioni non eccedano il perimetro della propria abitazione. In tale caso è buona norma che l'amministratore richieda al condomino copia della relazione tecnica e dei campi di visione delle videocamere installate.
- **Il controllo delle aree comuni ai fini SICUREZZA**: devono in tal caso essere adottate le misure previste dal Codice della Privacy con le relative comunicazioni agli organi di controllo. Questi i principali obblighi previsti dalla normativa sulla privacy:
    - Le telecamere devono essere segnalate con appositi cartelli;
    - Le registrazioni devono essere conservate per un periodo non maggiore a 24-28 ore (la necessità di un periodo più lungo deve essere verificata dal Garante Privacy);
    - Le telecamere devono riprendere solo le aree comuni;
    - I dati ripresi devono essere protetti con apposite misure di sicurezza;
    - L'installazione di tali apparecchi deve essere deliberata dall'assemblea con un numero di voti che rappresenti la maggioranza degli intervenuti e almeno la metà del valore dell'edificio. Alle apparecchiature di videosorveglianza sono equiparati i videocitofoni a cui sono applicate per analogia le regole di cui sopra, salvo che siano installati da persone fisiche per uso strettamente personale.

## SISTEMI INFORMATICI

Rientrano nella organizzazione anche i sistemi informatici utilizzati per l'attività e i vari collegamenti esterni. Quali sono i passi da fare?

- Procedere con un **elenco dei vari sistemi informatici** utilizzati (pacchetto office, eventuali applicativi specifici come programma di fatturazione, ecc.).
- Elencare i vari **utenti che utilizzano i programmi informatici e quali modalità di accesso hanno**;
- Elencare quali **sistemi** ANTIVIRUS o FIREWALL sono **utilizzati** e che tipo **di protezione** è stata attivata;
- Definire il tuo **sistema di salvataggio dei dati informatici**, frequenza e modalità di salvataggio;
- Se si utilizzano sistemi in Cloud avere chiaro **come vengono archiviati i dati e su quali server**, se sono residenti in territori italiani, europei o fuori dai confini europei;

## TIPOLOGIA DEI DATI TRATTATI [Finalità e scopi]

Un punto chiave della nuova privacy sarà stabilire con esattezza le finalità ovvero gli scopi per cui l'amministratore ha necessità di trattare e gestire alcuni dati nella sua azienda, in questo caso del **CONDOMINIO.**

Per fare questo un semplice passo è quello di predisporre una tabella (come quella indicata nel seguito) nella quale inserire gli ambiti, le tipologie di dati e le finalità che possono essere presenti nelle diverse attività aziendali:

| **AMBITO** | **TIPO DI DATO** | **FINALITÀ / SCOPI** |
|---|---|---|
| GESTIONE ASSEMBLEA | Nominativi, indirizzi, numeri di telefono, situazione debitoria, dati bancari | Gestione amministrativa / Contabilità |
| COMUNICAZIONE IN BACHECA | Nomi e cognomi lavoratori, dati bancari | Gestione Contabile/ Amministrativa |
| VIDEOSORVEGLIANZA | Filmati / Riprese | Sicurezza |
| CONSULENTE INFORMATICO / PROVIDER | Tutti i dati societari gestiti a livello informatico, gestione password | Archivio e backup dati |

Ovviamente si tratta solo di un esempio che si dovrà completare con dati specifici e relative finalità.

## VALUTAZIONE DEI RISCHI

Dopo aver fatto la mappatura delle varie tipologie di dati e le finalità si dovrà stabilire una modalità relativa la valutazione dei rischi. Ovvero **indicare in termini numerici qual è il livello di probabilità e quindi il RISCHIO che un dato possa essere violato**.

I rischi sono identificati in funzione:

- del tipo di dato
- di come viene effettuato il trattamento
- di chi effettua il trattamento
- di quale impatto/conseguenze il rischio può avere.

Al fine di poter oggettivare la Valutazione del Rischio, le sue componenti vengono suddivise nelle seguenti macro tipologie.

**RISCHIO DI AREA** (che dipende dal luogo dove gli strumenti sono ubicati)
Tale rischio è legato sostanzialmente:

- Al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti);
- Alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

Di seguito viene appunto effettuata una valutazione del grado di rischio che incombe sulla gestione e trattamento dei dati, siano essi cartacei o elettronici.

| EVENTO | DESCRIZIONE | GRAVITÀ | MISURE DI PREVENZIONE ATTUATE | MISURE DI PREVENZIONE DA ATTUARE |
|---|---|---|---|---|
| Accessi da parte di terzi non autorizzati | Nel normale orario di lavoro si accede in ufficio facendosi riconoscere al videocitofono. Le persone esterne sono accolte all'ingresso e non hanno possibilità di accedere autonomamente ai documenti cartacei o informatici. | 2 | Il personale esterno è sempre accompagnato da personale dell'ufficio. Non è possibile accesso autonomo da parte di terzi. | Nessuna |
| Asportazione e furto di strumenti informatici | Lo studio è dotato di allarme perimetrale e volumetrico. La ditta XXX effettua il controllo esterno ... | 2 | Regole di comportamento e controllo giornaliero. | Nessuna |
| Eventi distruttivi naturali, dolosi o accidentali | Incendio: nei locali sono presenti sistemi antincendio ... | 1 | Verifica semestrale estintori da parte di ditta specializzata. | Nessuna |
| Guasti o malfunzionamenti (imianto elettrico, climatizzazione, ...) | Impianto a norma ... Incendio: nei locali sono presenti sistemi antincendio ... | 1 | Verifica semestrale estintori da parte di ditta specializzata. | Nessuna |
| ... | | | | |

Sulla base del risultato della valutazione dei rischi si dovrà stabilire l'eventuale piano di azioni o di mantenimento della situazione conforme.

## RISCHIO LEGATO AL COMPORTAMENTO DEGLI OPERATORI

- Furto di credenziali di autenticazione;
- Carenza di consapevolezza, disattenzione o incuria;
- Comportamenti sleali;
- Errore umano.

## RISCHIO LEGATO AGLI STRUMENTI UTILIZZATI

- Azione di virus informatici;
- Spamming o altre tecniche di sabotaggio;
- Malfunzionamento o degrado degli strumenti;
- Accessi esterni non autorizzati;
- Intercettazione di informazioni in rete.

## LETTERE DI CONSENSO E DI RISERVATEZZA

Occorre prima fare un doveroso distinguo tra cosa significa **CONSENSO** e cosa significa **RISERVATEZZA**.

Il **CONSENSO** sarà necessario verso tutti coloro di cui si trattano dei dati specifici. Quindi di nuovo parliamo di:

- Dipendenti dello studio di amministrazione condominiale
- Consulenti
- Fornitori
- Clienti

Si dovranno a questo punto preparare delle specifiche lettere di consenso da inviare a tutti i soggetti di cui sopra spiegando loro le tipologie di dati trattati, le finalità e gli scopi. Dovranno essere firmate e restituite, e soprattutto fare attenzione ad archiviarle e tenerle sempre e costantemente disponibili.
**Si dovrà ripetere questa operazione ogniqualvolta si aggiunge un dipendente, si cambia un fornitore o si aggiunge un cliente**.

La **RISERVATEZZA** invece si riferisce più ad una tutela dell'amministratore, ovvero al fatto di garantire che i dati aziendali, le informazioni, il know-how non vengano trafugati dai dipendenti o collaboratori, sia durante le attività lavorative che eventualmente a fine rapporto.
Si deve predisporre quindi una specifica lettera da far firmare ad ogni dipendente e collaboratore con la quale vengono definite in modo chiaro le regole di riservatezza aziendale.

## DIRITTO ALL'OBLIO

**Questo è un requisito nuovo nel panorama Privacy.** Nel momento in cui il rapporto di lavoro viene a cessare, un dipendente si licenzia o viene cambiato un fornitore, oppure un cliente cessa di essere cliente, tutti i dati sia in forma **cartacea** che **informatica** dovranno essere eliminati. Si dovrà quindi comunicare a questi soggetti le modalità di eliminazione e distruzione dei propri dati al fine di rispettare appunto questo diritto all'oblio.

## TUTELA DEI MINORI DI ETÀ INFERIORE AI 16 ANNI

Se si amministrano stabili di associazioni o scuole che accolgono personale minore con età inferiore ai 16 anni, si dovrà pensare a mettere in atto sistemi per verificare l'età delle persone e per raccogliere il consenso dei genitori o dei tutori per l'elaborazione dei dati personali ove si rendesse necessario.

## REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

Il Registro dei Trattamenti dei Dati Personali è uno degli adempimenti introdotti con il Regolamento europeo sulla privacy. È quel documento attraverso il quale i soggetti che trattano i dati personali raccolgono tutte le informazioni relative alla gestione dei trattamenti che essi svolgono.
Il registro può essere creato in forma scritta o elettronica e al suo interno dovranno essere riportati i dettagli delle attività svolte in merito ai dati personali. Ad esempio dovranno essere indicate le modalità e gli scopi del trattamento, le categorie di dati trattati, le misure di sicurezza adottate, etc. Deve essere sempre aggiornato provvedendo a tenere traccia di ogni eventuale nuovo trattamento dei dati o di modifiche a quelli esistenti.

In molti casi redigere questo documento è obbligatorio, in generale però predisporre un registro dei trattamenti è sempre consigliato per:

- tener sempre traccia delle attività svolte ed avviare così un'attività di mappatura dei dati trattati (ad es. annotare nuovi trattamenti, modifiche nei destinatari extra-UE, cessione di trattamenti, etc.);
- poter mostrare al Garante Privacy (se lo richiede) la propria conformità al principio di responsabilizzazione richiesto dal GDPR.

## DATI PER LA SICUREZZA (Allegato al registro anagrafe)

L'amministratore deve:
...omissis.. 6) curare la tenuta del registro di anagrafe condominiale contenente le generalità dei singoli proprietari e dei titolari di diritti reali e di diritti personali di godimento, comprensive del codice fiscale e della residenza o domicilio, i dati catastali di ciascuna unità immobiliare, nonché ogni dato relativo alle condizioni di sicurezza delle parti comuni dell'edificio. Ogni variazione dei dati deve essere comunicata all'amministratore in forma scritta entro sessanta giorni.

In virtù di detto nuovo dato normativo si può ritenere che **l'amministratore è tenuto a raccogliere in un unico contenitore tutti i dati riguardanti gli impianti e le condizioni di sicurezza del fabbricato** che a loro volta sono indicate come obbligatorie dalle singole e specifiche norme che riguardano appunto detti impianti.

## Alla fine i documenti più importanti che si dovranno produrre sono:

- Informativa
- Nomine del Titolare, del Responsabile e degli Incaricati
- Elaborazione del DDMS (Documento Descrittivo delle Misure di Sicurezza)
- Mappatura e Valutazione dei rischi in materia di Privacy e trattamento dei dati
- Predisposizione lettere di riservatezza dei dati aziendali
- Lettere di consenso dipendenti, clienti e fornitori
- Registro dei trattamenti dei dati personali
- Dati per la sicurezza