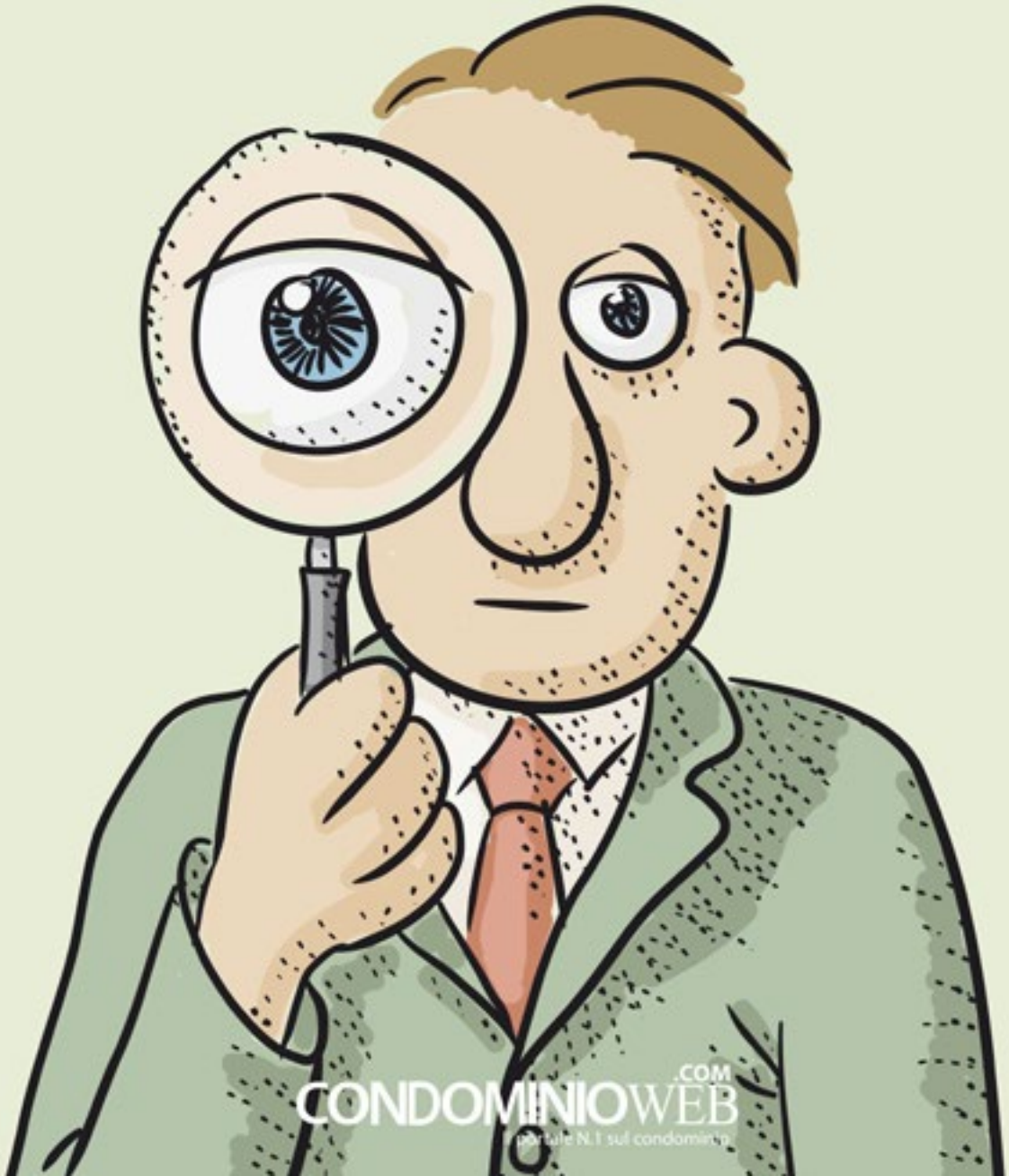
PRIVACY IN CONDOMINIO

LE NOVITÀ INTRODOTTE DAL GDPR 2018

I QUESITI DEGLI AMMINISTRATORI E LE RISPOSTE DEGLI ESPERTI

IVANO ROSSI

Esperto nel settore della privacy in ambito condominiale



CONDOMINIOWEB.COM

Prima edizione - Giugno 2018

Isbn: 9788899197384

Autore: **Ivano Rossi**

Email: info@condominioweb.com

Sito Web: www.condominioweb.com

Coordinatore Editoriale

Dott. Ivan Meo

Cell. 340.24.64.960 - press@condominioweb.com

Copertina, impostazione grafica e impaginazione: Alessandro Cavalieri

PRIVACY IN CONDOMINIO

LE NOVITÀ INTRODOTTE DAL GDPR 2018

I QUESITI DEGLI AMMINISTRATORI E LE RISPOSTE DEGLI ESPERTI

IVANO ROSSI

Esperto nel settore della privacy

CONDOMINIOWEB.COM

INDICE

LA PRIVACY
ALCUNE CONSIDERAZIONI INTRODUTTIVE

LA PRIVACY

ALCUNE CONSIDERAZIONI INTRODUTTIVE

1. BREVE STORIA DELLA NASCITA DELLA PRIVACY

La nascita del diritto alla privacy inizia a fine Ottocento, si sviluppa in maniera importante nel Novecento, per poi "esplodere" all'inizio del XXI sec., sia sotto il profilo del controllo, sia sotto il profilo della diffusione e della prolificazione dell'informazione di massa.

Gli albori della storia del diritto alla privacy sono nell'articolo "**Right to privacy**", apparso il 15 dicembre 1890 sulla Harvard Law Review (rivista giuridica degli Stati Uniti), ad opera di due giovani avvocati bostoniani, Samuel D. Warren e Louis D. Brandeis, i quali analizzarono in maniera molto precisa e articolata il rapporto tra il diritto di informare ed essere informati e la riservatezza.

L'articolo seppe distinguere tra: il diritto ad informare e a essere informati senza quasi limiti se l'oggetto dell'informazione è una persona pubblica, perché tale informazione ha una giustificazione democratica soprattutto se la persona in questione ha una carica che comporta responsabilità pubbliche; il diritto alla riservatezza se la persona è un normale privato cittadino, perché in tal caso manca l'interesse pubblico legittimo nel conoscerne i comportamenti.

Questo è il momento in cui, in letteratura, si fa coincidere la nascita del diritto alla privacy negli Stati Uniti inteso come elemento di equilibrio fra riservatezza e informazione.

In Europa, diversamente dagli USA, si è verificata una storia di stati totalitari, che hanno agito da controllori nei confronti dei cittadini: per tale ragione, in Europa si è sviluppata, dal punto di vista storico, una sensibilità diversa nei confronti della privacy. L'esperienza europea del Novecento è stata quella di un controllo delle informazioni sui cittadini da parte degli Stati: il vero problema, in tale contesto, non erano gli articoli diffamatori della stampa, ma la volontà del potere e dello Stato di conoscere la comunicazione interpersonale.

Storicamente, quindi, la comunicazione come nuova tecnologia ha avuto due effetti diversi: negli Stati Uniti ha dato luogo all'analisi nuova e moderna del rapporto tra riservatezza e diritto a informare e a essere informati, mentre nel continente europeo ha posto nuovi problemi di potenzialità di controllo dell'autorità pubblica sui comportamenti dei cittadini al fine di controllarli.

Pertanto, l'approccio europeista, diverso da quello oltre oceano, ha portato gli stati europei alla firma a Roma il 4 novembre 1950 della Convenzione Europea dei Diritti dell'Uomo (CEDU), creando un sistema di tutela internazionale dei diritti dell'uomo.

Altro passo significativo all'interno dell'ordinamento CEDU è la Convenzione di Strasburgo n. 108 del 1981 con la quale il trattamento "automatizzato" dei dati dei cittadini viene sottoposto a regole specifiche di garanzia, tra cui le regole del consenso al trattamento da parte dei cittadini e l'obbligo di non trasferire i dati nell'ambito di ordinamenti che non garantiscono la protezione dei dati personali.

Il primo contributo dell'Unione Europea in materia di privacy, successivo alla CEDU, dobbiamo attendere il 1995 con l'emanazione della cosiddetta **Direttiva Madre**.

Con la Direttiva del Parlamento europeo e del Consiglio n. 95/46/CE la Comunità europea ha introdotto un complesso sistema di regole che devono governare i trattamenti, anche non automatizzati, di dati personali.

La Direttiva 95/46/CE del 24 ottobre 1995 viene anche definita "Direttiva madre", proprio in quanto costituisce il testo di riferimento, a livello europeo, in materia di protezione dei dati personali. A tal fine, la direttiva fissa limiti precisi per la raccolta e l'utilizzazione dei dati personali e chiede a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della protezione di tali dati, il che ha condotto poi alla nascita delle Autorità nazionali di protezione dati.

L'articolo 29 della Direttiva 95/46 istituisce, inoltre, uno specifico Gruppo per la tutela delle persone che è composto da un rappresentante della Autorità di controllo designate da ciascuno Stato membro e da un rappresentante della Commissione. Il Gruppo, che si riunisce a Bruxelles ogni bimestre, ha un carattere consultivo nei confronti di tutti gli atti adottati a livello comunitario che possono incidere sulla protezione dei dati.

Obiettivo della Direttiva è essenzialmente quello di conformare la tutela delle libertà delle persone fisiche con l'esigenza della libera circolazione dei dati tra Stati membri, strumentale a sua volta all'esercizio delle libertà di circolazione delle persone, beni e servizi all'interno del mercato e quindi al suo buon funzionamento.

Lo scopo prioritario della Direttiva è quello di creare una disciplina armonica di tutela dei dati personali per evitare la formazione di un eccessivo scarto nei livelli di tutela dei diritti e delle libertà fondamentali, che può ostacolare non solo la salvaguardia delle posizioni soggettive, ma anche l'esercizio di una serie di attività economiche su scala comunitaria. Tuttavia le disposizioni normative contenute nella direttiva 95/46/CE sono tali da vincolare gli Stati membri a conformarsi ad esse, lasciando, comunque, ai legislatori nazionali significativi margini di adattamento, specie per quanto riguarda la disciplina delle deroghe in specifici settori.

DIRETTIVA MADRE 95/46/CE	
Autorità Garanti indipendenti	Compito della vigilanza sulla conformità delle leggi alla Direttiva 95/46/CE.
Working Party 29	Costituzione di un gruppo di lavoro composto dalle autorità nazionali.
Legittimazione leggi nazionali	Legittimazione dell'applicazione di leggi nazionali diverse all'interno dell'CE in materia di protezione dei dati (mutuo riconoscimento): indirettamente, questa agevolazione tra stati europei si è rivelata anche una barriera di protezione dell'Unione Europea verso i paesi extraeuropei, che per operare in Europa devono applicare le diverse leggi nazionali.
Legge 675 del 31 dicembre 1996	Testo legge di recepimento Direttiva 95/46/CE sul trattamento dei dati, istituisce l'Autorità Garante in Italia.
Decreto Legislativo 30 giugno 2003 n. 196	Detto "Codice Privacy", Testo Unico ai fini della razionalizzazione del complesso di norme in materia di trattamento dei dati personali.

IN EVIDENZA

In Italia fu creata la figura del Garante per la protezione dei dati personali in qualità di autorità amministrativa indipendente istituita dalla legge n. 675 del 31 dicembre 1996 (cosiddetta legge sulla privacy), per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali.

Il Garante si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali.

Il Garante si occupa, tra l'altro, di:

- controllare che i trattamenti di dati personali siano conformi a leggi e regolamenti e, eventualmente, prescrivere ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento;
- esaminare reclami e segnalazioni nonché decidere i ricorsi presentati ai sensi dell'articolo 145 del Codice in materia di protezione dei dati personali;
- vietare in tutto od in parte, ovvero disporre il blocco del trattamento di dati personali che per la loro natura, per le modalità o per gli effetti del loro trattamento possano rappresentare un rilevante pregiudizio per l'interessato;
- adottare i provvedimenti previsti dalla normativa in materia di dati personali, tra cui, in particolare, le autorizzazioni generali per il trattamento dei dati sensibili;
- promuovere la sottoscrizione dei codici di deontologia e di buona condotta in vari ambiti (credito al consumo, attività giornalistica, ecc.);
- segnalare, quando ritenuto opportuno, al Governo la necessità di adottare provvedimenti normativi specifici in ambito economico e sociale;
- partecipare alla discussione su iniziative normative con audizioni presso il Parlamento;
- formulare i pareri richiesti dal Presidente del Consiglio o da ciascun ministro in ordine a regolamenti ed atti amministrativi suscettibili di incidere sulle materie disciplinate dal Codice;
- predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy da trasmettere al Parlamento e al Governo;
- partecipare alle attività comunitarie ed internazionali di settore, anche quale componente del Gruppo Articolo 29 e delle Autorità comuni di controllo previste da convenzioni internazionali (Europol, Schengen, Sistema informativo doganale);
- curare la tenuta del registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37 del Codice in materia di protezione dei dati personali;

- curare l'informazione e la sensibilizzazione dei cittadini in materia di trattamento dei dati personali, nonché sulle misure di sicurezza dei dati;

coinvolgere i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale…

2. REGOLAMENTO EUROPEO 2016/679 – GDPR (General Data Protection Regolation)

Il Regolamento Europeo 2016/679, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 è entrato in vigore il 25 maggio 2016 e dovrà essere applicato da ogni stato membro dal 25 maggio 2018.

Esso è obbligatorio e vincolante in tutti i suoi elementi e si applica a tutte le persone fisiche e giuridiche che si trovano in Europa e non necessità di un atto interno di recepimento da parte del singolo Stato membro al fine di farlo confluire nelle fonti dell'ordinamento giuridico nazionale.

Il Regolamento Europeo 2016/679 è direttamente applicabile in Italia ed è azionabile dinanzi all'Autorità garante per la protezione dei dati personali o ai giudici nazionali.
Prima procedere oltre e per comprendere meglio la terminologia che verrà utilizzata, di seguito un sintetico glossario con riferimenti al condominio:

Descrizione	Applicabilità al Condominio	Soggetti coinvolti al rispetto
Regolamento Europeo 2016/679 – GDPR: regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE	SI	Condominio – Amministratore del condominio – Incaricati/ Autorizzati del condominio e dell'amministratore – altri responsabili esterni
ANC Autorità Nazionale di Controllo: autorità competente per la gestione dei reclami o di eventuali violazioni al GDPR e delle norma nazionali in materia di protezione dei dati	SI	Possono rivolgersi tutti coloro che ritengono violati i propri diritti privacy: tutte le persone fisiche i cui dati personali sono trattati dal condominio
Codice Privacy: D.Lgs 30 giugno 2003, n. 196 - "Codice in materia di protezione dei dati personali"	SI	Sono chiamati al rispetto tutti i soggetti che trattano dati personali: condominio, amministratore, responsabile interno e esterno
Dati personali: qualunque informazione relativa a una persona fisica, identificata o identificabile, anche indirettamente, attraverso altre informazioni, ivi compreso un numero di identificazione personale	SI	Nome, cognome, codice fiscale, interno e scala dell'abitazione, consumi idrici/riscaldamento, dati catastali, recapiti telefonici, email, fotogrammi, targhe automobilistiche, etc ...
Dati biometrici: dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca attraverso il loro trattamento	SI	Utilizzo di strumenti per il rilevamento di immagini facciali, impronta digitale, sistemi di videoripresa cosiddetti intelligenti
Dati sanitari: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute	SI	Referti del pronto soccorso in caso di sinistro, documentazione per l'abbattimento di barriere architettoniche

Dati sensibili: dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati o associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dati personali idonei a rilevare lo stato di salute e la vita sessuale.	SI	Busta paga di un dipendente con ritenute sindacali, indicazioni riferite a handicap, cambio di sesso
Finalità: scopo determinato, esplicito e legittimo che viene perseguito dal titolare del trattamento	SI	Amministrazione, contabilità, sicurezza, gestione del bene comune
Trattamento dei dati: qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione di dati personali, anche se non registrati in una banca dati	SI	Tutte le operazioni effettuate con i dati personali dal momento della raccolta (ad esempio subentro, nuova locazione, acquisizioni immagini, passaggio di consegne...), alla distruzione (cancellazione dati da supporti informatici, distruzione archivi cartacei – per l'amministratore non coincide con il passaggio di consegne dei documenti condominiali)
Titolare del trattamento: persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza	SI	Condominio, amministratore all'interno del suo studio

Responsabile del trattamento: persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento	SI	Amministratore del condominio – altri responsabili esterni su nomina del titolare del trattamento dei dati o dal responsabile del trattamento se autorizzato dal titolare
Incaricato: persona fisica autorizzata a compiere operazioni di trattamento sulla base delle istruzioni ricevute dal titolare e/o dal responsabile, ove designato	SI	Dipendente del condominio, collaboratori di studio dell'amministratore
Interessato: persona fisica a cui si riferiscono i dati personali	SI	Tutte le persone fisiche i cui dati sono trattati dal condominio
Informativa: documento contenente le informazioni che il titolare deve fornire all'interessato per chiarire se quest'ultimo è obbligato o meno a rilasciare i dati personali, le conseguenze di un eventuale rifiuto al rilascio dei dati personali, quali sono le finalità e le modalità del trattamento, i soggetti che entrano in contatto con i suoi dati personali, come circolano i dati personali e in che modo esercitare i diritti riconosciuti dal GDPR	SI	Documento obbligatorio da consegnare o rendere disponibile a tutti gli interessati i cui dati personali sono oggetto di trattamento da parte del condomino
Consenso: Manifestazione di volontà libera, specifica e informata dell'interessato con cui questi accetta espressamente che i suoi dati siano fatti oggetto di trattamento	SI	E' necessario raccoglierlo quando vengo effettuati trattamenti dei dati diversi dalle finalità per i quali sono stati raccolti
Misure di sicurezza: Complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di sicurezza	SI	Il Condominio, l'amministratore e gli altri responsabili esterni sono tenuti a garantire la sicurezza dei dati trattati non solo a livello informatico ma anche cartaceo

Responsabile Protezione dei dati (DPO): Professionista esterno o interno alla azienda, che il titolare nomina al fine di avere al suo interno un punto di riferimento esperto privacy	SI/NO	IL Responsabile della protezione dei dati deve essere nominato, dal titolare e/o dal responsabile del trattamento dei dati, nei casi in cui il trattamento effettuato richieda monitoraggio regolare e sistematico degli interessati su larga scala.
Valutazione Impatto Privacy (VIP) – Data Protection Impact Assessment (DPIA): E' la valutazione che il titolare del trattamento deve effettuare ogni qualvolta possa esserci un rischio elevato per i diritti e le libertà delle persone interessate	SI	Il Condominio e/o l'amministratore quale responsabile del trattamento dei dati ogni qual volta intendano eseguire un trattamento di dati che possa mettere a rischio i diritti e le libertà degli interessati devono effettuare una valutazione di impatto. Un sistema di videosorveglianza o il controllo degli accessi in un complesso residenziale possono essere oggetto di VIP;
Registro dei trattamenti: registro delle attività di trattamento, conservato dal titolare	SI/Consigliato	Seppur obbligatorio nel caso di presenza di oltre 250 dipendenti, è fortemente consigliato redigere il registro ove elencare i trattamenti dei dati effettuati. E' uno strumento utile per verificare, sulla base dei vari trattamenti, le misure di sicurezza adottate o da adottare e in caso di ispezione.
Registro delle violazioni: documento in cui riportare le violazioni dei dati personali subite nel tempo	SI	Strumento utile in caso di verifica da parte dell'AdC per dimostrare il rispetto del GPDR relativamente alle misure di sicurezza

Comunicazione violazione dati personali (Data Breach): comunicazione delle violazione dei dati personali all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza salvo che non sia probabile che la violazione presenti un rischio per i diritti degli interessati. In caso di violazione subita dal responsabile del trattamento, esso è tenuto a darne tempestiva comunicazione al titolare	SI	Qualora il Condominio subisca una violazione dei dati personali trattati, ad esempio le immagini di un impianto di videosorveglianza, esso è tenuto a dare comunicazione all'Autorità di controllo entro 72 ore. Allo stesso modo l'amministratore che subisce una violazione deve dare tempestiva comunicazione al titolare, il Condominio, che provvederà a segnalarlo all'Autorità. Se esiste un pericolo per le libertà e i diritti degli interessati, il titolare, quindi il condominio, è tenuto alla comunicazioni a ogni interessato
Amministratore di Sistema (AdS): professionista che, in ambito informatico, gestisce e manutiene un impianto di elaborazione dati	Dipende	Se il Condominio, al suo interno, è datato di un rete informatica per l'elaborazione dei dati e demanda a un soggetto la gestione/manutenzione, come ad esempio la gestione delle password, backup, registrazione log, accessi remoti, occorre la nomina specifica ad amministratore di sistema. Lo stesso l'amministratore che utilizza un tecnico esterno che ha accesso alle impianto informatico, dovrà nominare ad AdS il tecnico incaricato

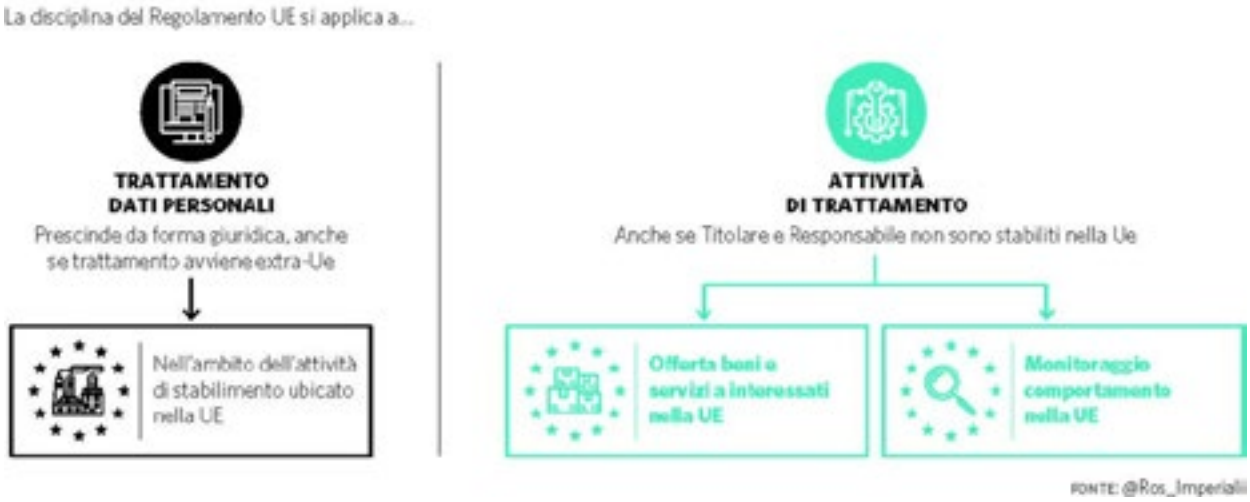

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
GUIDA AL NUOVO
REGOLAMENTO EUROPEO
IN MATERIA DI PROTEZIONE
DEI DATI PERSONALI
Più diritti e più opportunità per tutti
Il Regolamento porterà significative innovazioni non solo per i cittadini, ma anche per le aziende, gli enti pubblici, le associazioni, i liberi professionisti


Cittadini più garantiti
Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (data breach).
INFORMATIVA
Informazioni più chiare e complete sul trattamento
CONSENSO
Consenso, strumento di garanzia anche on line
TRATTAMENTI AUTOMATIZZATI
Limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato di dati
NUOVI DIRITTI
Più tutele e libertà con il diritto all'oblio e il diritto alla portabilità dei dati
TRASFERIMENTO DATI
Garanzie rigorose per il trasferimento dei dati al di fuori dell'Ue
DATA BREACH
Obbligo di comunicare i casi di violazione dei dati personali (data breach)
Novità per le imprese e gli enti
Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate.
NORMATIVA UNICA
Un unico insieme di norme per tutti gli Stati dell'Unione europea
ACCOUNTABILITY
Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili
CERTIFICAZIONI E CODICI DEONTOLOGICI
Semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione

Il Regolamento Europeo 2016/679 quindi si applica ai dati personali delle persone fisiche, è diretto a fornire un quadro giuridico più coerente e solido, per assicurare l'omogeneità delle modalità del trattamento dei dati nei vari Stati membri.
A questo proposito analizziamo l'ambito di applicazione del GDPR.

Ambito di applicabilità	Rispetto al Condominio
Oggetto e finalità: il GDPR si applica a tutte le persone fisiche indipendentemente dalla loro nazionalità o residenza, interessati, e non alle persone giuridiche. Se il trattamento dei dati ha carattere personale o domestico, il GDPR non si applica.	Il Condominio, quale titolare del trattamento, così come l'amministratore, quale responsabile del trattamento, trattando dati personali di persone fisiche sono obbligati al rispetto del GDPR. Si precisa che un indirizzo email nome.cognome@nomeazienda.it è un dato personale e non un dato di un soggetto giuridico
Applicazione materiale: si applica ai trattamenti effettuati con strumenti automatizzati e non. Il paragrafo 2, articolo 2 indica le esclusioni, ed esattamente quando: - non ricade nel diritto dell'Unione; - è effettuato dallo Stato membro in virtù delle disposizioni specifiche di politica estera e sicurezza; - è effettuato per finalità personali o domestiche; - è svolto da autorità pubbliche per finalità di sicurezza pubblica e prevenzione dei reati.	Il Condominio, l'amministratore e gli altri eventuali responsabili, sono soggetti al GDPR in quanto trattano dati di persone fisiche sia con strumenti automatizzati, sia in modo cartaceo e sono soggetti al diritto dell'Unione. Trattano, altresì, i dati per finalità diverse da quelle domestiche e/o personali
Applicazione territoriale: il GDPR si applica sempre nei seguenti casi: - sul territorio dell'Unione; - indipendentemente dallo stabilimento del titolare, quindi anche se al di fuori dell'UE, se il trattamento riguarda dati di persone fisiche residenti in Europa per scopi commerciali o monitoraggio dei comportamenti; - se il titolare/responsabile è stabilito in Europa e il trattamento è materialmente effettuato in paesi extra UE;	Il Condominio, l'amministratore ed eventuali altri responsabili devono applicare il GDPR in quanto sono stabiliti sul territorio dell'Unione. Qualora vengano nominati responsabili stabiliti fuori dell'Unione, ad esempio servizi in cloud, il titolare dovrà verificare che il trattamento effettuato rispetti il GDPR

IN EVIDENZA
Quando il condominio o l'amministratore incaricano un altro soggetto al trattamento di dati il cui stabilimento è al di fuori dell'Unione Europea, questi dovranno verificare tra l'altro, che egli abbia nominato un rappresentante che si trovi in Italia. Ed esempio se si utilizza un provider cloud con stabilimento in Albania, dovrà essere verificato che questo abbia nominato un suo rappresentante privacy in Italia.



3. PRINCIPI - LICEITÀ - CONSENSO - DIRITTI DEGLI NTERESSATI

L'importanza che il legislatore europeo ha voluto dare ai principi e ai diritti degli interessati si comprende dall'impianto sanzionatorio di riferimento (art. 83 par. 5 lett. a) Reg. 2016/679). A differenza del D. Lgs 196/2003 il loro mancato rispetto, prevede l'intervento immediato dell'Autorità di controllo attraverso azioni *"effettive, proporzionate e dissuasive"*.

Di contro, in fase di ispezione, prima di irrogare una sanzione, vengono tenute in giusta considerazione le operazioni eseguite dal titolare del trattamento o dal responsabile del trattamento per il rispetto del GDPR e la tutela dell'interessato. Infatti ricordiamo che all'Autorità di controllo ha tutta una serie di poteri correttivi che può applicare prima di irrogare una sanzione (art. 58 par. 2 Reg. 2016/679). Dipenderà molto dall'atteggiamento del titolare e del responsabile del trattamento.

Per comprendere meglio e successivamente capire come operare per dimostrare il comportamento pro attivo del titolare del trattamento dei dati e del responsabile del trattamento dei dati, esaminiamo i principi e i diritti degli interessati

Liceità - correttezza - trasparenza	Il Condominio e l'amministratore possono trattare i dati degli interessati solo in modo lecito, vale a dire conforme alla legge. Quando parliamo di legge non si intende solo la normativa privacy, ma tutte le fonti del diritto. Già l'art. 15 del Codice della Privacy richiama in tutto e per tutto la disciplina civilistica in materia di risarcimento del danno da illecito (art. 2050 c.c., assimilando la disciplina del trattamento dei dati personali a quella dello svolgimento di attività pericolose). Secondo il GDPR il titolare del trattamento e/o il responsabile del trattamento dati, condominio-amministratore-altri responsabili, tratterranno in modo lecito i dati: a) se è stato raccolto il consenso per i trattamenti diversi dalle finalità previste; b) se il trattamento effettuato rispetta il rapporto giuridico sottostante (condominio/amministratore: gestione del bene comune, erogazione di servizi condominiali, amministrazione e contabilità, sicurezza...); c) se il trattamento è necessario per adempiere ad un obbligo legale (rispetto del D.Lgs 81/08, anagrafica condominiale...) d) se il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica (comunicazione a terzi di informazioni/dati di carattere personale in caso di urgenza per la sicurezza fisica della persona o delle persone residenti nel condominio); e) se il trattamento è necessario per il perseguimento di un legittimo interesse (accertamenti per il recupero dei crediti condominiali, mancata cancellazione di dati personali per la difesa in un giudizio...). L'interessato deve poter conoscere in qualsiasi momento quali dati è in possesso il titolare e il responsabile ed estrarne copia
Finalità determinate, esplicite e legittime	Significa che i dati trattati dal condominio e/o dall'amministratore devono seguire specifiche finalità, devono avere uno scopo ben preciso. Questo deve essere dichiarato e deve essere conforme alla legge. Sarà importante quindi che le finalità siano circoscritte e definite all'interno dell'informativa, documento obbligatorio da consegnare all'interessato

Adeguatezza, pertinenza, limitazione	Questi tre concetti si applicano secondo le necessità per il rispetto delle finalità per i quali i dati sono trattati *(minimizzazione dei dati)*. Significa che il condominio deve essere in possesso solo dei dati necessari per l'espletamento delle attività specifiche condominiali, non altri (periodi di vacanza degli interessati, preferenze calcistiche, orientamenti politici o religiosi...)
Esattezza dei dati	I dati in possesso del condominio devono essere sempre corrispondere all'interessato ed essere rettificati tempestivamente in caso di inesattezza rispetto alle finalità per i quali sono trattati. Questo implica un aggiornamento costante e periodico (anagrafe condominiale è bene chiedere conferma dei dati periodicamente e almeno una volta l'anno)
Periodo di conservazione	I dati devono essere conservati per un periodo di tempo limitato e comunque secondo le finalità per i quali sono stati trattati. Generalmente, salvo particolari casi, si fa riferimento alla prescrizione decennale, ex art. 2946 C.C.
Sicurezza dei dati	Il condominio-l'amministratore o altri responsabili sono tenuti a garantire la sicurezza dei dati trattati "mediante misure tecniche organizzative adeguate", compreso il trattamento da parte di soggetti non autorizzati, la perdita o la distruzione seppur accidentale

IN EVIDENZA
Il paragrafo 2 dell'articolo 5 del Regolamento Europeo 2016/679 riporta espressamente che il titolare del trattamento dei dati "è competente" per il rispetto dei principi e deve essere in grado di comprovarlo. Poche righe che attribuiscono una enorme responsabilità in testa al titolare del trattamento, il condominio, che non essendo assimilabile a un'impresa, ma bensì composto da una pluralità di soggetti contitolari degli stessi diritti, non ha al suo interno una struttura e un organico ben definito ma ha, al contrario, un suo legale rappresentante, l'amministratore di condominio. Pertanto la responsabilità del rispetto dei principi del GDPR sarà in testa all'amministratore inteso, in questo caso, come rappresentante del titolare del trattamento. Non necessariamente l'amministratore potrà avere le competenze necessarie per il rispetto pieno del Regolamento Europeo 2016/679 ed è pertanto consigliato l'affiancamento di un consulente privacy da individuare con oculatezza

Diritto di accesso ai propri dati personali	L'interessato, che abbiamo visto essere in ambito condominiale la persona fisica che gode di diritti reali o di godimento, ma anche la persona che occasionalmente accede in un'area videoripresa, ha il diritto di accesso ai dati che lo riguardano e di cui il titolare è in possesso. In caso di richiesta e dopo aver accertato l'identità dell'interessato, l'amministratore è tenuto a comunicare all'interessato i dati personali trattati

Diritto all'informazione	Il Regolamento Europeo UE 2016/679 obbliga il titolare del trattamento a informare gli interessati in modo chiaro, coinciso e trasparente. L'informativa, oltre a indicare l'identità del titolare, quindi i dati del condominio e del suo rappresentante legale, dovrà riportare una serie di informazioni come di seguito indicate:	
	Le finalità del trattamento;	Adempimento degli obblighi di legge, amministrazione e contabilità, sicurezza, gestione del bene comune
	Le categorie dei dati personali trattati;	Dati personali comuni, identificativi, fiscali
	I destinatari o le categorie di destinatari a cui i dati personali dell'interessato sono stati o saranno comunicati;	Consulente del lavoro, ced, fiscalista
	Il periodo di conservazione dei dati oppure i criteri utilizzati per la determinazione del periodo	Articolo 2946 c.c.
	Diritto di richiedere la rettifica o la cancellazione dei dati personali o la limitazione o opposizione al loro trattamento	La rettifica o la cancellazione dei soli dati non necessari per l'espletamento degli obblighi di legge o per le finalità proprie del condominio può essere esercitato in qualsiasi momento. Esempio: in caso di vendita di un immobile, l'ex-proprietario potrà chiedere solo il blocco dei dati per ulteriori trattamenti ma non la cancellazione in base ai tempi di conservazione e alla necessità di eventuali successivi controlli contabili futuri
	Il diritto di proporre reclamo all'Autorità di controllo	Nel caso in cui l'interessato dovesse ritenere di essere oggetto di un trattamento illecito o di mancato rispetto dei sui diritti potrà rivolgersi all'Autorità Garante
	Se i dati non sono stati raccolti presso l'interessato, occorre fornire informazioni delle loro origini	Passaggio consegne da latro amministratore, conservatoria, catasto urbano…

	L'esistenza di un processo decisionale automatizzato e sulla logica	Emissione solleciti di pagamento per crediti superiori a una soglia o in base al tempo di ritardo rispetto alla data di scadenza della rata
Diritto di rettifica	Il titolare del trattamento dei dati deve rettificare o cancellare tutti i dati personali affetti da errore	
Diritto di limitazione del trattamento	In caso di mancata legittimazione da parte dell'interessato alla richiesta di cancellazione dei dati personali, esso può chiedere la limitazione del trattamento dei dati. L'interessato può chiedere la limitazione nei casi in cui: • il trattamento è illecito; • i dati non sono più necessari per il perseguimento delle finalità indicate dal titolare; • esiste un motivo legittimo prevalente (ex procedimento legale in corso);	
Diritto alla portabilità dei dati	• l'interessato può chiedere il trasferimento dei propri dati personali da un titolare "originario" a un altro titolare. Il titolare "originario" a: • fornire una copia dei dati personali dell'interessato in un formato elettronico, strutturato in modo tale che possa essere letto da un pc e possa essere riutilizzato (in ambito condominiale questo vale nei confronti degli interessati ma anche tra amministratori durante il passaggio di consegne. Non sarà più sufficiente consegnare la documentazione solo in formato cartaceo); • salvare i propri dati personali su un device personale.	
Diritto di opposizione	In realtà se il condominio e l'amministratore si attengono alle finalità proprie della gestione condominiale, gli interessati, intesi come i titolari di diritti reali o di godimento, non potranno opporsi al trattamento dei loro dati in quanto necessari ai fini della gestione condominiale e per gli obblighi di legge	

IN EVIDENZA

Rispetto alla Direttiva Madre 95/46/CE, il GDPR introduce l'obbligo da parte del titolare del trattamento dei dati ad agevolare l'esercizio dei diritti dell'interessato ai sensi dell'articolo 12, paragrafo 2. Questo obbligo può non essere adempiuto nel caso in cui il titolare non sia in grado di identificare l'interessato.

In ambito condominiale, l'amministratore può rifiutarsi di far accedere all'anagrafica condominiale, alla contabilità o rispondere alla richiesta di invio di un consuntivo nel caso in cui non dovesse essere certo del titolo del soggetto che chiede dette informazioni. Può, in questi casi chiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato e quindi il diritto di accesso.

Si ricorda che il titolare è tenuto a espletare le richieste avanzate dell'interessato nell'esercizio dei suoi diritti sanciti ex articoli 15-22 senza ingiustificato ritardo e, comunque, non oltre un mese dal ricevimento della richiesta. Trascorso questo termine senza riscontro da parte del titolare, l'interessato è legittimato ad adire l'Autorità di controllo e/o la giustizia ordinaria.

Il Garante con provvedimento del 18 maggio del 2006 doc. Web n. 1297626 riconosce il Condominio come *"Titolare del trattamento dei dati"* cioè colui che assume *"le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"* (art. 4 c. 2 lett. f D.Lgs 196/2003).

L'amministratore può essere nominato in veste di responsabile del trattamento ai sensi degli artt. 4, comma 1, lett. g), e 29 D.Lgs 196/2003 vale a dire colui che per conto del titolare svolge i compiti assegnati utilizzando i dati personali raccolti dal titolare secondo determinate finalità. Quindi già dal 2006 il Garante chiariva i compiti, i ruoli e le incombenze per il trattamento dei dati nel mondo condominiale.

Con il GDPR, l'approccio al trattamento dei dati cambia. Il Titolare del trattamento dei dati rimane il Condominio che per sua natura, non essendo dotato e organizzato con struttura propria, demanda all'amministratore, quale professionista esterno, quasi tutti i trattamenti.

A differenza del D. Lgs 196/2003, che alla data della presente stesura siamo in attesa del decreto legislativo di armonizzazione con il Regolamento Europeo 2016/679, il GDPR amplia le responsabilità e i doveri del titolare e del responsabile del trattamento dei dati. In particolare il titolare del trattamento, il condominio, (art. 24 Reg. UE 2016/679), attraverso l'assemblea e/o il suo legale rappresentante, dovrà, a seconda del contesto e delle finalità dei trattamenti, valutare i rischi per i diritti e le libertà delle persone fisiche mettendo in atto misure tecniche e organizzative adeguate per garantire e dimostrare il rispetto del Regolamento.

Dovrà:

- far predisporre una informativa adeguata rispetto al GDPR da far pervenire o mettere a disposizione degli interessati (chiunque detiene un diritto reale o di godimento e i cui dati sono in possesso del condominio o ad esempio di chiunque accede in uno stabile dotato di videosorveglianza);
- rispettare e far rispettare i principi del regolamento e i diritti degli interessati (art. 5 e artt 12 a 22 Reg. UE 2016/679);
- trattare i dati secondo liceità (art. 6 Reg. UE 2016/679);
- provvedere in forma scritta alle nomine dei responsabili al trattamento e/o autorizzati (amministratore di condominio, fornitori di servizi che utilizzano dati personali, videosorveglianza, dipendenti del condominio, ect);
- predisporre misure di sicurezza adeguate qualora vengano svolti trattamenti presso il condominio (ad esempio un archivio cartaceo, registrazioni immagini, smistamento corrispondenza e raccolta pacchi, monitoraggio degli accessi come lettura targhe, ect);
- valutare l'impatto privacy prima di ogni nuovo trattamento (ed esempio installazione di impianto di videosorveglianza, apertura varchi da remoto e registrazione accessi, utilizzo videocitofono da remoto, ect);

È consigliabile, quindi che il condominio si doti di un proprio disciplinare con il richiamo esplicito ad alcuni articoli e adempimenti previsti dal GDPR, da rendere disponibile alla compagine condominiale e all'amministratore di condominio nella veste di responsabile del trattamento dati (art. 4, par. 1, p, 8 Reg. UE 2016/679).

Di contro, essendo in realtà il condominio un ente di gestione, demanda la maggior parte dei trattamenti all'amministratore, nella persona di un professionista o società esterna al condominio con **l'obbligo**, non più la facoltà, di nominarlo come responsabile del trattamento (art. 28 Reg. UE 2016/679). Il titolare, quindi i condomini stessi, nella sua nomina quale amministratore dello stabile per i compiti richiamati dall'articolo 1130 del Codice Civile o per altri servizi proposti nell'offerta presentata, dovranno verificare sotto la loro responsabilità diretta, che il professionista nominato presenti *"garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca i diritti dell'interessato"* (condomini, inquilini, ect).

L'amministratore, quale responsabile del trattamento, dovrà:

- trattare i dati solo secondo le finalità e le modalità del suo mandato e dettate dalla legge (obbligo giuridico);
- garantire la riservatezza delle persone da lui autorizzate al trattamento dei dati (collaboratori);
- adottare e dare evidenza delle misure di sicurezza presenti presso il suo studio;
- assistere il titolare del trattamento, il condominio, nel garantire i diritti degli interessati;
- assistere il titolare del trattamento, il condominio, al rispetto delle misure di sicurezza dei dati trattati, ai rapporti con l'Autorità di controllo, Garante, a valutare l'impatto di nuovi trattamenti;
- al rispetto dei diritti degli interessati da parte del titolare;
- consentire le ispezioni da parte del titolare per la verifica del rispetto del GDPR;
- informare immediatamente il titolare se uno dei trattamenti violi il regolamento o vi siano violazione dei dati in suo possesso.

Occorre prestare particolare attenzione al rispetto dell'articolo 28 paragrafo 2 ed esattamente:

Art. 28 par. 2 Reg. 2016/679

"Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche".

Se non seguiranno specifiche indicazioni da parte del Garante, questo paragrafo obbliga l'amministratore di condominio a chiedere autorizzazione preventiva ai condomini, ad esempio, per poter trasferire su un provider cloud i dati dei condomini stessi in quanto quest'ultimo si configurerebbe come responsabile esterno nominato dall'amministratore, responsabile esterno nominato dal condominio quale titolare del trattamento. Il provider cloud non necessariamente deve un terminal server o una macchina virtuale appositamente creata. Può essere anche lo spazio web messo a disposizione dell'amministratore dalla software house che fornisce il programma di contabilità per poter pubblicare documenti condominiali, estratti conto personali e così via.

CONDOMINIO **Titolare del trattamento** **artt. 4 (7) – 24 GDPR**	**AMMINISTRATORE DI CONDOMINIO** **Responsabile del trattamento** **artt. 4 (8) – 28 GDPR**
• Predisposizione informativa adeguata in rispetto del GDPR; • rispettare e far rispettare i principi del regolamento e i diritti degli interessati (art. 5 e artt. 12 a 22 Reg. UE 2016/679); • trattare i dati secondo liceità (art. 6 Reg. UE 2016/679); • provvedere in forma scritta alle nomine dei responsabili al trattamento e/o autorizzati; • predisporre misure di sicurezza adeguate qualora vengano svolti trattamenti presso il condominio; • verificare che i responsabili del trattamento nominati presentino garanzie sufficienti per il rispetto del regolamento e garantiscano i diritti degli interessati; • formazione delle persone che hanno accesso a dati personali; • valutare l'impatto privacy prima di ogni nuovo trattamento; • comunicare all'Autorità di controllo eventuali violazione di dati anche se a carico del responsabile del trattamento dei dati entro 72 ore dalla conoscenza. In caso di rischio per la libertà e i diritti fondamentali degli interessati, comunicare la violazione anche a quest'ultimi;	• Trattare i dati solo secondo le finalità e le modalità del suo mandato e dettate dalla legge (obbligo giuridico); • garantire la riservatezza delle persone da lui autorizzate al trattamento dei dati (collaboratori); • adottare e dare evidenza delle misure di sicurezza presenti presso il suo studio; • assistere il titolare del trattamento, il condominio, nel garantire i diritti degli interessati; • assistere il titolare del trattamento, il condominio, al rispetto delle misure di sicurezza dei dati trattati, ai rapporti con l'Autorità di controllo, Garante, a valutare l'impatto di nuovi trattamenti; • rispetto dei diritti degli interessati da parte del titolare; • consentire le ispezioni da parte del titolare per la verifica del rispetto del GDPR; • informare immediatamente il titolare se uno dei trattamenti violi il regolamento o vi siano violazione dei dati in suo possesso; • nel caso di violazione del regolamento e determinazione delle finalità e dei mezzi del trattamento, viene considerato un titolare del trattamento

4. NOMINE E AUTORIZZAZIONI AL TRATTAMENTO

Il GDPR impone al titolare che decide di nominare un responsabile del trattamento dei dati ad avvalersi solo di quei soggetti che hanno i requisiti per garantire il rispetto del Regolamento (art. 28 par. 1). In particolare il responsabile dovrà garantire l'adozione di adeguate garanzie per lo svolgimento dei trattamenti.

La nomina a responsabile del trattamento dei dati deve essere in forma scritta e deve contenere quanto previsto dall'articolo 28 del GDPR. Non deve essere confusa come una semplice formalità, ma al contrario deve essere un contratto vincolante tra le parti. In mancanza, il titolare risponde personalmente delle violazioni commesse da eventuali responsabili al trattamento.

Il responsabile del trattamento, se non espressamente autorizzato dal titolare, non può nominare altri responsabili. Eventuali altri responsabili nominati dal responsabile, comunicati e autorizzati dal titolare, sono soggetti agli stessi obblighi legislativi e contrattuali a cui è soggetto il responsabile nominato direttamente dal titolare.

IL Regolamento UE 2016/679 prevede la figura dell' "autorizzato al trattamento". Il titolare del trattamento è obbligato a redigere un atto di autorizzazione che contenga l'ambito del trattamento, l'autorizzazione al trattamento dei dati oltre alle istruzioni per il trattamento stesso, per l'uso dei dispositivi e per il rispetto delle misure di sicurezza da adottare. Il "principio di responsabilizzazione" (art. 5 par. 2 Reg. UE 2016/679) prevede che il titolare o il responsabile al trattamento debba prevedere l'adozione di misure di sicurezza atte a garantire pro-attivamente l'osservanza del regolamento. In questo assume particolare importanza la formazione degli addetti al trattamento così come previsto dall'articolo 29. Occorrerà quindi istruire gli addetti, documentando la formazione, verificando e aggiornando annualmente le procedure, mantenendo il requisito della formazione stessa.

AZIONI	SPECIFICHE	ESEMPI PRATICI
Stesura e sottoscrizione atto di autorizzazione	Ambito del trattamento consentito; Istruzioni sulle operazioni di trattamento Istruzioni sulle misure di sicurezza	Contabilità e amministrazione; Procedure sulle operazioni da eseguire sui dati – manuale operativo; Indicazioni del back-up, duplicazione e cancellazione dati, utilizzo internet, aggiornamento antivirus...
Obbligo formativo	Documentare sessione di formazione	Sottoscrizione scheda partecipazione alla formazione, indicazione degli argomenti, test di valutazione finale
Verifica annuale	Profilo autorizzazione Aggiornamento istruzioni Mantenimento requisito formativo	Verifica se la persona svolge gli stessi incarichi Verifica se le istruzioni sono adeguate ai trattamenti ed eventuale aggiornamento Documentazione formazione e test di valutazione

In attesa del decreto legislativo di armonizzazione tra il Codice Privacy e Regolamento Europeo UE 2016/679, di seguito alcuni esempi sintetici di nomina a responsabile del trattamento dell'amministratore del condominio (ex art. 28 GDPR), nomina di responsabile esterno (ex art. 29 D. Lgs 196/2003), nomina autorizzato elaborati appositamente per essere utili strumenti di lavoro all'amministratore di condominio

NOMINA A RESPONSABILE DEL TRATTAMENTO

Artt. 4 e 28 Regolamento UE 2016/679

Condominio <NOME_CONDOMINIO> - <INDIRIZZO_CONDOMINIO> - CF <CODICE_FISCALE> in qualità di Titolare del Trattamento, del Regolamento Generale sulla protezione dei dati personali – Regolamento UE 2016/679 (RPD o GDPR) *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.*

Premesso che:

- per «**RPD o GDPR**» si intende il Regolamento sulla Protezione dei Dati o General Data Protection Regulation;
- per «**responsabile del trattamento**» si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- per «**trattamento**» si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- per «**dato personale**» si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale";
- per «**autorizzazione**» si intendono le operazioni alle quali è autorizzato l'incaricato del trattamento in base alle mansioni ricoperte;
- per «**funzioni da amministratore di sistema**» si intendono lo svolgimento di tutte quelle attività dedicate alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali;
- che il Condominio su intestato è il *Titolare del trattamento dei dati personali*;
- il **Responsabile del trattamento**, fornisce garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

tutto ciò premesso, con la presente viene:

NOMINATO RESPONSABILE DEL TRATTAMENTO

Il Sig. <"NOME_AMMINISTRATORE"> C.F. <CF__PIVA>

Il Responsabile del trattamento, operando nell'ambito dei principi stabiliti dal Regolamento UE 2016/679, è vincolato agli impegni di seguito riportati.

Finalità del trattamento – Il Responsabile si impegna a trattare i dati personali del Condominio titolare del trattamento solo per le finalità connesse allo svolgimento delle attività oggetto del rapporto contrattuale, con divieto di qualsiasi altra diversa utilizzazione.

Riservatezza – Il Responsabile ai sensi dell'articolo 28 paragrafo 3, lett.b) garantisce che tutte le persone interne incaricate al trattamento sono state espressamente autorizzate con impegno di riservatezza.

Modalità del trattamento – Il Responsabile nell'ambito delle attività previste dal contratto con il Titolare ha autonomia di procedere con trattamenti sia cartacei che automatizzato.

Sicurezza del trattamento – Il Responsabile dovrà gestire i sistemi informatici, nel quale risiedono i dati del Titolare, adottando tutte le misure tecniche e organizzative in base al rischio.

Assistenza al titolare – Il Responsabile assiste il Titolare fornendogli idonea assistenza al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste di esercizio dei diritti da parte degli interessati.

Durata e termine del trattamento – Il Responsabile è tenuto ad aggiornare e/o distruggere i dati personali detenuti, tenuto conto degli obblighi legali di conservazione e per un periodo non superiore a quello necessario per gli scopi del trattamento.

Ispezioni – Il responsabile è tenuto a mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento comprese attività di revisione, ispezione.

Attività di valutazione d'impatto privacy – Il Responsabile deve assistere il Titolare, se richiesto, nelle attività di Valutazione d'impatto privacy.

Il Responsabile del trattamento

_____

Per accettazione della nomina

ATTO DI NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

ART. 29 D.LGS N. 196/2003

Condominio <NOME_CONDOMINIO> - <INDIRIZZO_CONDOMINIO> - CF <"CODICE_FISCALE"> in qualità di Titolare del Trattamento dei dati personali, dopo una attenta valutazione in merito alla sussistenza dei requisiti di esperienza, capacità e affidabilità di cui all'art. 29 comma 2° del Decreto Legislativo 196/2003:

NOMINA DEL FORNITORE A RESPONSABILE DEL TRATTAMENTO

ai sensi dell'art. 29 D.Lgs n.196/2003

Il Sig./la Sig.ra _____
__C.F. _____

Il Responsabile esterno del trattamento, operando nell'ambito dei principi stabiliti dal Regolamento UE 2016/679, e tenuto conto di quanto stabilito dalla disciplina nazionale si impegna a:

- compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione della disciplina in tema di protezione dei dati personali;
- adottare e rispettare le misure di sicurezza indicate e predisposte dal titolare del trattamento;
- individuare e nominare gli incaricati del trattamento impartendo loro per iscritto le istruzioni necessarie per un corretto, lecito e sicuro trattamento di dati;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del D.lgs. 30 giugno 2003, n. 196;
- monitorare periodicamente l'adeguatezza delle misure di sicurezza adottate;
- di effettuare il trattamento dei dati forniti solo ed esclusivamente in ragione delle finalità per le quali sono stati affidati;

Il Responsabile del Trattamento dichiara di aver preso conoscenza dei compiti che gli sono affidati, della gratuità della nomina e di essere a conoscenza di quanto stabilito dalla disciplina vigente in materia di protezione dei dati personali.

Dopo attenta lettura di ogni singolo punto, con la sottoscrizione della presente, il Responsabile esterno accetta la nomina.

Il Responsabile del trattamento

_____

Per accettazione della nomina

AUTORIZZAZIONE DEL DIPENDENTE

Egr. Sig. ….<AUTORIZZATO>

premesso che

lei è alle dipendenze del **Condominio <NOME_CONDOMINIO>- <INDIRIZZO_ CONDOMINIO> - CF <"CODICE_FISCALE">** in qualità di Titolare del Trattamento dei dati personali

oppure

lei è alle dipendenze dello Studio di Amministrazioni condominiali **<NOME_COGNOME – SOCIETA'> - CF <"CODICE_FISCALE">** in qualità di Titolare del Trattamento dei dati personali

e svolge attività di ….....

Essendo stato assunto per lo svolgimento delle mansioni assegnate da contratto, che prevedono il trattamento di dati personali, e che detta attività, tra le altre, è disciplinata dal Regolamento UE 2016/679 e dalle norme di settore,

che per effetto del Regolamento UE 2016/679 il titolare del trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti cloro che sono stati autorizzati al trattamento dei dati personali

TUTTO CIÒ PREMESSO

Lei è autorizzato al trattamento dei dati personali.

La presente autorizzazione ha effetto solo per le banche dati e per le operazioni di cui alla scheda che viene allegata alla autorizzazione e che ne forma parte integrante.

Il trattamento dovrà essere limitato a quanto necessario e indispensabile per l'adempimento delle sue mansioni osservando con scrupolo e in modo inderogabile le norme di legge, regolamenti interni, ordini di servizio, il manuale della sicurezza ad uso degli autorizzati al trattamento dei dati e comunque alle istruzioni impartite anche verbalmente dal titolare del trattamento dei dati.

Gli obblighi sopra descritti fanno parete integrante della prestazione lavorativa e pertanto sono da lei dovuti in base al vigente contratto di lavoro e nel caso di violazione saranno applicate le sanzioni previste dal contratto medesimo.

La presente autorizzazione è subordinata esclusivamente alla durata del rapporto di lavoro o fino a revoca espressa da parte del titolare del trattamento dei dati.

L'Autorizzato

_____

Per accettazione della nomina

5. REGISTRO DEI TRATTAMENTI

Il registro dei trattamenti è uno strumento utile per definire e censire i trattamenti svolti. Molto spesso, specie in piccole realtà, presi dalla routin non ci si sofferma sui reali trattamenti eseguiti e rimane difficile censirli durante una ispezione dell'Autorità di controllo o, in caso di responsabile, di semplice richiesta da parte del titolare.

L'articolo 30 del Regolamento prevede la obbligatorietà del registro dei trattamenti nel caso di aziende con oltre 250 dipendenti o in caso di trattamenti di categorie di dati particolari o rischio elevato per gli interessati.

Il condominio e l'amministratore difficilmente sono chiamati a redigere il registro dei trattamenti. È comunque fortemente consigliato in quanto se da un lato il titolare è obbligato a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al regolamento, dall'altro deve conoscere e avere a portata di mano l'elenco dei trattamenti eseguiti.

È per questo motivo che il Garante incentiva in ogni caso la redazione del registro dei trattamenti.

6. MISURE DI SICUREZZA – NOTIFICA VIOLAZIONI – COMUNICAZIONE AGLI INTERESSATI

L'articolo 32 del Regolamento UE 2016/679 intitolato *"Sicurezza del trattamento"* è il primo articolo della Sezione 2 dedicata alla *"Sicurezza dei dati personali"*. Nel GDPR è rafforzata l'introduzione delle misure di sicurezza e delle misure di tutela e garanzia dell'interessato nel trattamento dei suoi dati sin dalla progettazione degli strumenti utilizzati (art. 25).

Il regolamento prevede misure di sicurezza adeguate da adottare in relazione alla valutazione dei rischi. Il titolare e il responsabile del trattamento dei dati sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione, la cifratura; misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni; la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico.

Le misure vanno contemperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento.

Il condominio, seppur titolare, sono poche le reali situazioni di trattamento dati diretto. Alcuni esempi potrebbero essere la videosorveglianza, la rilevazione degli accessi e così via. Ma la maggior parte dei trattamenti vengono demandati all'amministratore del condominio. Sarà pertanto quest'ultimo, sempre nella duplice veste di legale rappresentante del titolare e responsabile del trattamento, a doversi preoccupare di quali misure di sicurezza adottare.

Per far questo dovrà avere prima ben chiari i trattamenti effettuati e per ognuno valutare il rischio e definire la misura di mitigazione adeguata.

È possibile iniziare rispondendo a queste semplici domande:

- Che cosa può andare storto?
- Quanto può essere dannoso?
- Quante volte può succedere?

Con questo semplice metodo oltre a individuare le diverse tipologie di rischio, si assegna a questi un diverso livello di gravità in base all'entità del danno e della sua possibilità di ripetersi nel tempo. Sulla base di queste informazioni vengono decise ed implementate le misure di sicurezza.

I rischi possono essere suddivisi in tre macro aree in funzione della loro natura:

1. Comportamento degli operatori: rischi riconducibili all'azione diretta dell'operatore che tratta i dati;
2. Eventi relativi agli strumenti: rischi di natura tecnica informatica;
3. Eventi relativi al contesto: rischi riconducibili a cause diverse dalle precedenti solitamente di tipo fisico e non riconducibili agli operatori.

Ancora oggi può essere ritenuto valido, unicamente come traccia non essendo più esaustivo ai fini del principio di responsabilizzazione del titolare del trattamento (accountability), le indicazioni riportate nell'allegato B del D. Lgs 196/2003 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1557184).

La tabella sottostante è un esempio, secondo il D. Lgs 196/2003, delle misure obbligatorie che può essere utilizzata come base di partenza per identificare le prime misure di sicurezza adeguate al rischio secondo il principio di accountability del GDPR.

Elenco alcuni rischi		**Gravità**
Comportamenti degli operatori	sottrazione di credenziali di autenticazione	Media
	carenza di consapevolezza, disattenzione o incuria	Media/Alta
	comportamenti sleali o fraudolenti	Bassa
	errore materiale	Media
	assenza	Media
Eventi relativi agli strumenti	azione di virusi informatici o di programmi scuscettibili di recare danno	Media/Alta
	spamming o tecniche di sabotaggio	Alta
	malfunzionamento, indisponibilità o degrado degli strumenti	Media
	accessi esterni non autorizzati	Media
	intercettazione di informazione di rete	Alta
	accessi non autorizzati a locali/reparti ad eccesso ristretto	Bassa
	sottrazione di strumenti contenenti dati	Media
Eventi relativi a contesto	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, etc.), nonché dolosi, accidentali o dovuti a incuria, guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Bassa
	errori umani nella gestione della sicurezza fisica	Media

Ancora oggi può essere ritenuto valido, unicamente come traccia non essendo più esaustivo ai fini del principio di responsabilizzazione del titolare del trattamento (accountability), le indicazioni riportate nell'allegato B del D. lgs. 196/2003.

(http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1557184).

La tabella sottostante è un esempio, secondo il D. lgs. 196/2003, delle misure obbligatorie che può essere utilizzata come base di partenza per identificare le prime misure di sicurezza adeguate al rischio secondo il principio di accountability del GDPR.

Descrizione misure di sicurezza adottate	Obbligatoria	Consigliata in base al rischio
Definizione di profili di accesso al Database elettronico	**X**	
Attivazione di un sistema di autenticazione costituito da un codice identificativo (userid) e una parola chiave conosciuta solamente dall'incaricato (password)	**X**	
Attivazione della modalità Stand-by sui pc dopo 15 minuti di mancanza di input	**X**	
Installazione di un programma antivirus su ogni pc	**X**	
Installazione di un firewall hardware sul server	**X**	
Salvataggio giornaliero di una copia di sicurezza del Database (back-up)	**X**	
Adozione di tecniche di business continuity		**X**
In caso di cloud salvataggio giornaliero di una copia di sicurezza su disco fisico		**X**
Sollevamento da terra del server		**X**
Gruppo di continuità		**X**

Quando il trattamento "*può*" assumere un rischio elevato per i diritti e le libertà delle persone fisiche occorrerà, prima di effettuarlo, eseguire una Valutazione di Impatto Privacy (VIP) (art. 35 Reg. UE 2016/679), vale a dire analizzare attraverso un documento gli specifici rischi che comporta quel trattamento e le precauzioni di alto livello da adottare per procedere al trattamento stesso. La VIP è obbligatoria se la tipologia di trattamento rientra in quelle che verranno elencate dal Garante in apposito elenco pubblico ovvero quelle elencate e non soggette a VIP (art. 35 par. 4 e 5 GDPR).

Apparentemente può sembrare che il condominio non si trovi mai in questa situazione, ma da una lettura attenta dell'articolo 35 troviamo al paragrafo 3 lettera c) *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"*. Ci sono diverse realtà condominiali dove viene posta una telecamera che riprende una galleria commerciale interna all'edificio, oppure complessi residenziali con all'interno centri commerciali, negozi, scuole, uffici postali ove accedono non solo i condomini ma un numero imprecisato di persone estranee alla vita condominiale o centri commerciali costituiti in condominio. In questi casi l'amministratore dovrà preoccuparsi, magari con l'aiuto di un consulente privacy, di eseguire una valutazione di impatto documentando il processo e le decisioni con le quali sono state vagliate e adottate le misure di sicurezza al rischio.

CONTENUTI DELLA VIP		
Regolamento UE 2016/679	**Contenuti**	**Caso di videosorveglianza sistematica su larga scala in condominio**
Considerando 90 - Articolo 35	Descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, interesse legittimo perseguito da titolare	Videosorveglianza degli accessi e degli spazi comuni del Condominio/Complesso residenziale per fini di sicurezza interna e protezione del patrimonio
	Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità	Il monitoraggio verrà eseguito esclusivamente secondo le finalità perseguite con l'uso di un impianto di videosorveglianza come meglio descritto nella relazione tecnica, e in rispetto del provvedimento del Garante dell'8 aprile 2010
	Valutazione dei rischi per i diritti e le libertà degli interessati	Potendo il trattamento incidere sulla vita privata delle persone occorre procedere alla valutazione dei rischi di perdita o accesso fraudolento ai sistemi di registrazione anche da personale dipendente
	Misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento	Elencazione delle varie misure adottate sulla base del singolo rischio individuato

Una novità rispetto alla Direttiva Madre 95/46/CE è la comunicazione della violazione dei dati personali all'Autorità di controllo. Anche il questo il condominio e l'amministratore non posso esimersi di rispettare l'articolo 33 del GDPR, che prevede appositi comportamenti e tempi entro i quali comunicare al Garante fatti che hanno compromesso l'integrità dei dati personali trattati (Data breach). Il titolare del trattamento deve, entro 72 ore da quando ne ha notizia, notificare all'Autorità di controllo la violazione dei dati. Questo significa che il titolare entro detto termine deve identificare la violazione, la revisione della documentazione, l'adozione di procedure che mitigano il danno arrecato e notificare all'Autorità di controllo il data breach. Nel caso in cui la violazione ponga a rischio i diritti e le libertà fondamentali dell'interessato, occorre comunicare anche a questi la violazione subita.

Naturalmente è possibile mettere in atto misure di sicurezza adeguate per poter essere esentati da

tale obbligo come ad esempio sistemi di cifratura dei dati che rendono gli stessi inutilizzabili da terzi oppure vengo poste immediatamente in essere misure di sicurezza che assicurano l'assenza di rischi per gli interessati.
Riveste particolare importanza è l'esecuzione di una analisi dei rischi non solo delle vulnerabilità informatiche, ma con l'individuazione di tutte quelle situazioni in cui le procedure utilizzate potrebbero compromettere la sicurezza delle informazioni tra cui la gestione documentale cartacea.

7. DIRITTO AL RISARCIMENTO – SANZIONI – POTERI AUTORITA' DI CONTROLLO

Con il Regolamento UE 2016/679 sia il titolare che il responsabile del trattamento dei dati sono chiamati a risarcire direttamente l'interessato del danno subito, materiale o immateriale, in caso di trattamento illecito dei suoi dati.

Il responsabile, l'amministratore o altro responsabile esterno, risponde del danno nei confronti dell'interessato se:

- non ha adempiuto agli obblighi del Regolamento;
- non ha adempiuto alle indicazioni documentate impartite dal titolare.

IN EVIDENZA
Qualora il titolare o il responsabile sono responsabili del danno causato ad un interessato del trattamento, il titolare e il responsabile sono "responsabili in solido". *Il titolare e il responsabile sono esonerati dalla responsabilità per il risarcimento dei danni solo se dimostrano che l'evento dannoso non è a loro imputabile.*

In merito alle sanzioni amministrative, con il GDPR il Garante europeo ha innalzato di molto il massimo edittale che può essere irrorato al titolare del trattamento. L'articolo 83 specifica due livelli di sanzioni con massimali diversi. Le sanzioni amministrative si applicano sia alle persone fisiche che alle imprese. L'irrogazione è da parte dell'Autorità d controllo e può sanzionare sia il titolare che il responsabile al trattamento dei dati.

DESCRIZIONE	*SANZIONE AMMINISTRATIVA*	*RESPONSABILITÀ CIVILE*	*SANZIONI ACCESSORIE*
Violazioni dei Principi Fondamentali Privacy (artt. 5 – 6 GDPR)	Fino a € 20 milioni o fino al 4% del fatturato se superiore	Responsabilità danni patrimoniali e no patrimoniali	Blocco dei trattamenti Blocco del trasferimento all'estero Revoca della certificazione privacy
Omesso consenso (art. 7 GDPR)			
Trattamento illecito dei dati sensibili e giudiziari ((art. 9 GDPR)			
Omessa o inidonea informativa all'interessato (artt. da 12 a 14 GDPR)			
Violazione dei diritti dell'interessato (artt. da 15 a 21 GDPR)			
Profilazione e trattamento automatizzato illecito o non autorizzato (art. 22 GDPR)			
Trasferimento dei dati personali all'estero illecito o non autorizzato (artt. da 44 a 49 GDPR)			
Violazione di disposizioni statali su specifici trattamenti (artt. da 85 a 91 GDPR)			
Omessa informazione o esibizione al Garante privacy (art. 51.1 GDPR)			
Inosservanza dei provvedimenti del Garante privacy (art. 58.2 GDPR)			

DESCRIZIONE	*SANZIONE AMMINISTRATIVA*	*RESPONSABILITÀ CIVILE*	*SANZIONI ACCESSORIE*
Omesso o inidoneo consenso on-line di minori (art. 8 GDPR)	Fino a € 10 milioni o fino al 2% del fatturato se superiore	Responsabilità danni patrimoniali e non patrimoniali	Blocco dei trattamenti Blocco del trasferimento all'estero Revoca della certificazione privacy
Non necessaria identificazione (art. 11 GDPR)			
Violazione dei principi privacy by design e by default (art. 25 GDPR)			
Violazione degli obblighi di contitolari, rappresentanti e responsabili del trattamento (artt. da 26 a 29 GDPR)			
Omessa istituzione e tenuta del registro di trattamenti (art. 30 GDPR)			
Omessa cooperazione con il Garante privacy (art. 31 GDPR)			
Omessa adozione di misure di sicurezza (art. 32 GDPR)			
Omessa notificazione e comunicazione di violazioni (artt. 33 e 34 GDPR)			
Omessa e inidonea valutazione d'impatto sulla protezione dei dati e consultazione preventiva (art. 35 e 38 GDPR)			
Violazione degli obblighi di designazione del DPO (artt. da 37 a 39 GDPR)			

Oltre allo strumento sanzionatorio, l'Autorità di controllo ha altri poteri per monitorare e rendere coerente l'applicazione del Regolamento. (art. 58)

POTERI DELL'AUTORITÀ DI CONTROLLO	*POTERI ESERCITATI NEL RISPETTO*
Poteri di indagine *Poteri correttivi e sanzionatori* *Poteri consultivi e autorizzativi* *Potere di agire o intentare un'azione in sede giudiziale o stragiudiziale in caso di violazione del Regolamento* *Potere di limitazione provvisoria o definitiva di un trattamento*	*Diritto del titolare e/o del responsabile di essere destinatario di una misura appropriata, necessaria, e proporzionata che tenga conto dello specifico caso* *Diritto di ogni persona di essere ascoltata prima dell'adozione di un provvedimento che rechi pregiudizio*

IN EVIDENZA

La normativa privacy ha una sua complessità nel metterla in opera, deve essere declinata alle diverse realtà in quanto copre trasversalmente svariati ambiti. Senza una preparazione e una attitudine alle procedure da seguire, rimane abbastanza complicato riuscire a districarsi sui passi necessari evitando ridondanze, irrigidimento di quelle che sono le operazioni giornaliere dello studio di amministrazione o dell'azienda o peggio ignorare degli adempimenti obbligatori. Per questo è importante chiedere un supporto esterno, almeno nelle prime fasi di implementazione.

Nella eventuale scelta del consulente, è consigliabile valutare i seguenti aspetti:

- *dimostrazione almeno documentale delle competenze in ambito privacy;*
- *dimostrazione delle competenze in ambito condominiale, possibilmente con capacità organizzative e conoscenza delle problematiche tipiche degli amministratori di condominio;*
- *conoscenza dei processi amministrativi e contabili;*
- *conoscenza degli strumenti informatici comunemente utilizzati;*
- *disponibilità a una consulenza costante;*
- *capacità di suggerire soluzioni a seconda delle problematiche e del budget a disposizione.*

La scelta di un consulente che ponga l'accento solo sulle possibili sanzioni che potrebbe essere irrorate dall'Autorità di controllo senza che ponga l'accento sulle soluzioni pratiche valutando di volta in volta i rischi, probabilmente non è la migliore.

8. DIPENDENTI

Aspetto importante e spesso trascurato, è il trattamento dei dati personali dei dipendenti.

L'amministratore di condominio può essere datore di lavoro di dipendenti di fabbricato e datore di lavoro dei propri dipendenti di studio.

In entrambi i casi è soggetto al rispetto della normativa privacy nei loro confronti relativamente alle informazioni che lì riguardano in virtù di un rapporto contrattuale sottostante. Gli aspetti importanti di cui l'amministratore dovrà tener conto sono:

- l'informativa sui trattamenti di dati personali;
- il consenso per il trattamento dei dati sensibili, e riferimento all'Autorizzazione Generale 1/2016 del Garante (doc. web 5800451);
- autorizzazione per il trattamento di immagini del dipendente;
- modalità ed eventuale comunicazione a terzi dei dati del dipendente;
- sicurezza dei canali di comunicazione dei dati personali;
- nomina dei responsabili esterni;
- procedura di archiviazione dei documenti cartacei;
- criteri dei tempi di detenzione dei dati.

Per meglio comprendere, di seguito una scheda esemplificativa

PRIVACY DATI PERSONALI DIPENDENTE	
Obbligo di comunicazione dell'informativa sui trattamenti di dati personali;	Documento da consegnare al dipendente ove indicare il titolare del trattamento dei dati, le finalità, le modalità di trattamento, le conseguenze di un rifiuto, eventuale comunicazione a terzi, diritti, riferimenti dell'Autorità di controllo
Consenso per il trattamento dei dati sensibili, con riferimento all'Autorizzazione Generale n. 1/2016;	Trattamento dei dati sensibili nei limiti dell'autorizzazione generale n. 1/2016 del Garante e minimizzazione dei dati raccolti
Modalità ed eventuale comunicazione a terzi dei dati del dipendente;	Consulente del lavoro, consulente fiscale, medico del lavoro, enti di previdenza, amministrazione finanziaria, società di credito e/o assicurative
Sicurezza dei canali di comunicazione dei dati personali;	I canali di trasmissione dei dati personali devono essere sicuri. Ad esempio la trasmissione delle buste paga da parte del consulente del lavoro non potrà avvenire con il semplice invio tramite email di un file pdf. Deve essere garantito un grado di sicurezza maggiore come ad esempio un file pdf criptato o protetto da password. Se viene utilizzato un canale web deve essere sicure, ad esempio protetto con un certificato SSL
Nomina dei responsabili esterni;	Dovranno essere nominati responsabili esterni (art. 28 GDRP) tutti i soggetti a cui i dati personali dei dipendenti saranno comunicati e trattati in assenza di un obbligo giuridico. Esempio consulente del lavoro e/o fiscalista, medico competente. Non occorre nomina verso enti previdenziali e assicurativi, agenzia delle entrate
Procedura di archiviazione dei documenti cartacei;	I documenti cartacei sono soggetti a normativa privacy al pari di quelli digitali. Dovranno essere previste delle procedure interne di archiviazione, individuati gli incaricati al trattamento
Criteri dei tempi di detenzione dei dati.	Devo essere stabiliti i tempi di conservazione dei dati del dipendente individuando un criterio che può essere diverso dalla prescrizione decennale previsa dal Codice Civile

Oltre al D. Lgs 196/2003 e al Regolamento UE 2016/679, per la privacy in ambito lavoristico non è possibile prescindere dall'articolo 4 dello Statuto dei lavoratori di seguito riportato:

Art. 4 Statuto dei lavoratori dopo la riforma D. Lgs 151/2015

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196

L'articolo 4 dello Statuto dei lavoratori introduce la tematica dei controlli a distanza facendo una espressa ammissione pur rimanendo preclusa qualsiasi finalità diversa rispetto a quelle chiaramente consentite dal legislatore, vale a dire:

- esigenze organizzative e produttive;
- sicurezza del lavoro;
- tutela del patrimonio aziendale.

Le vere novità della riforma le portano i commi 2 e 3 che introducono una netta distinzione tra strumenti di controllo e strumenti di lavoro. Per quest'ultimi non vi è la necessità di seguire la procedura codeterminativa introdotta dal comma 1.

Gli strumenti di lavoro, esclusi specificatamente dal comma 2, sono quelli utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Ad esempio son strumenti d lavoro i computer collegati alla rete aziendale, i telefonici, i tablet ma anche sistemi gps purché utilizzati con consentire l'attività lavorativa del dipendente.

In considerazione del rinvio al Codice della Privacy introdotto dal comma 3, l'amministratore di condominio, nella figura di datore di lavoro sarà tenuto a rispettare i seguenti principi:

PRINCIPI	
Principio di necessità	Riduzione al minimo dell'utilizzo dei dati personali e identificati del dipendente in relazione alle finalità perseguite con opportuna configurazione dei sistemi informatici di controllo
Principio di correttezza	Occorre rendere noto al lavoratore possibili monitoraggi attraverso gli strumenti dati in dotazione
Principio di pertinenza e non eccedenza	I trattamenti sui dati personali dei lavoratori devono essere svolti secondo le finalità determinate, legittime ed esplicite
Principio di trasparenza	Devono essere esclusi controlli informatici all'insaputa del lavoratore

Nuovamente l'informativa riveste un aspetto cruciale nel trattamento dei dati e deve essere consegnata o in ogni caso resa conoscibile al lavoratore anche tramite una rete entranet.

L'informativa rivolta ai dipendenti, oltre ad avere le caratteristiche già esposte nei capitoli precedenti, dovrà fare riferimento al sistema informatico nel suo complesso utilizzato dal dipendente per la propria attività lavorativa e che tramite lo stesso sarà possibile effettuare dei controlli a distanza. Sono esclusi controlli continuativi, costanti, prolungati e discriminatori.

I controlli che potranno essere effettuati sono per:

- verificare la corretta applicazione del regolamento privacy aziendale;
- il corretto utilizzo dei sistemi informatici (pc, tablet, rete internet...);
- garantire la sicurezza del sistema informatico;
- motivi tecnici o di manutenzione hardware.

Le risultanze dei controlli potranno essere comunicate al titolare, agli enti pubblici, all'autorità giudiziaria e di polizia oltre ai consulenti fiscali e legali.

Notizie aggiuntive informativa dipendenti (ex art. 4 L. 300/1970 3° comma)	
Strumenti informatici	Modalità d'uso, indicazione dei comportamenti tollerati e quali vietati, indicazione delle conseguenze disciplinari.
Controlli	Possibilità di controlli sul sistema informatico, periodicità degli stessi
Rispetto del diritto alla privacy	Indicazioni di quante e quali informazioni possono esser oggetto di memorizzazione, seppur temporanea, i tempi di conservazione.

Il legislatore europeo, attraverso l'articolo 88 del Regolamentato UE 2016/679, titolato *"Trattamento dei dati nell'ambito dei rapporti di lavoro"* lascia ad ogni singolo stato membro la possibilità di legiferare o concordare contratti collettivi per *"assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti d lavoro"*.

Quindi se da un lato non interviene direttamente con norme specifiche, dall'altro tende a garantire in ogni caso i diritti e le libertà derivanti dal trattamento dei dati personali dei lavoratori lasciando autonomia ai singoli stati europei.

8.1 POSTA ELETTRONICA – USO DI INTERNET

L'email è diventata uno strumento di uso comune ed è quello più utilizzato per comunicare e per trasmettere documenti.

L'indirizzo di posta elettronica può essere riferita a una funzione, *amministrazione@dominio.it*, generica, *info@dominio.it*, o personale *nome.cognome@dominio.it*.

Essendo la posta elettronica la porta virtuale con l'esterno, il datore di lavoro dovrà preoccuparsi di redigere un disciplinare d'uso, dettando le regole e i limiti circa le modalità del suo utilizzo.

Se l'account aziendale è generico, con la possibilità di lettura da parte di più soggetto, dovrà essere specificato l'uso per la trasmissione o ricezione di informazioni personali con l'avvertenza di cancellazione e richiami disciplinari.

In particolare se vengono creati email personali, il datore di lavoro dovrà definire da subito, oltre all'uso da parte del dipendente, anche le modalità di trattamento dei dati personali che potrebbero essere contenuti nelle comunicazioni trasmesse e ricevute nel corso del rapporto di lavoro sia dopo la sua cessazione prevedendo la cancellazione dell'account.

Il Garante obbliga il datore di lavoro a informare preventivamente il dipendente in merito alle finalità e delle modalità di raccolta e conservazione dei dati personali. È per questo che è fortemente consigliato inserire nel mansionario rivolto ai dipendenti anche questo aspetto. Nello stesso dovrà essere preso in considerazione anche la possibile assenza del dipendente e della necessità di accesso all'account attraverso altra persona appositamente autorizzata.

L'uso di internet deve essere regolamentato a salvaguardia della struttura informatica dell'azienda e dei dati contenuti nei server. È consigliabile limitare o vietare l'uso di internet per finalità personali, come il download di software o applicativi non riconducibili a necessità lavorative, l'acceso a determinati siti o social, alla posta elettronica personale, e comunque all'uso della rete aziendale per usi privati, attività ludiche o non pertinenti con l'attività lavorativa. Per prevenire questi atteggiamenti è possibile limitare l'hardware configurandolo in modo da impedire comportamenti contrari alla policy aziendale. Questo atteggiamento da parte del datore di lavoro può essere configurato come una misura di sicurezza.

8.2 VIDEOSORVEGLIANZA CON PRESENZA DI LAVORATORE SUBORDINATO

L'installazione di un impianto di videosorveglianza in un ambiente di lavoro da parte del titolare, è configurato come un controllo a distanza del lavoratore. L'articolo 4 dello Statuto dei lavoratori deve essere rispettato con ossequio se non si vuole incorrere alle sanzioni previste dallo Statuto e dal Codice Privacy.

In seguito alla riforma dell'articolo 4 dello Statuto dei lavoratori del 2015 (D.Lgs n.151 del 14.09.2015) sono state estese le finalità per poter installare sistemi di controllo a distanza, ed esattamente:

- per esigenze organizzative e produttive;
- per la sicurezza del lavoro;
- per la tutela del patrimonio aziendale

Pertanto il datore di lavoro, sia esso il condominio o l'amministratore di condominio all'interno del suo studio, può installare delle telecamere riconducendo i motivi a una o più di queste finalità.

Da una lettura integrale dell'articolo 4, questo è consentito salvo richiesta autorizzativa alla Direzione Territoriale del Lavoro, oggi Ispettorato Nazionale del Lavoro. Pertanto in caso di condominio, dopo la delibera di approvazione della realizzazione di un impianto di videosorveglianza e prima della sua realizzazione, occorrerà presentare istanza presso l'ispettorato.

In giurisprudenza una delle maggiori sentenze di riferimento, Cass., Sez. III pen., 12 novembre 2013, n. 4331, ha statuito che è necessaria l'autorizzazione preventiva delle DTL anche se l'impianto non è messo in funzione. *"In tema di impianti audiovisivi di controllo a distanza dei lavoratori, l'idoneità dell'impianto a ledere il bene giuridico protetto è sufficiente ad integrare il reato, anche se l'impianto non è messo in funzione, poiché, configurandosi come un reato di pericolo, la norma sanziona a priori l'installazione, prescindendo dal suo utilizzo o meno".*

Lo stesso Ministero del Lavoro e delle Politiche Sociali, in data 01 giugno 2016 prot. 37/0011241/MA007.A.001.10742, è intervenuto rendendo un parere in merito ad accertamenti ispettivi e aspetti sanzionatori riguardanti impianti audiovisivi installati senza accordo sindacale o autorizzazione ai sensi dell'art. 4, comma 1, legge n. 300/1970: *".....Il legislatore ha previsto in maniera chiara che il mancato rispetto della norma in materia di videosorveglianza è punito con ammenda da € 154 a € 1.549 o arresto da 15 giorni ad un anno (art. 38 della legge n. 370/1970), salvo che il fatto non costituisca reato più grave. Pertanto, qualora nel corso dell'attività ispettiva, l'ispettore riscontri l'installazione di impianti audiovisivi in assenza di uno specifico accordo sindacali ovvero in assenza dell'autorizzazione rilasciata da parte della Direzione del lavoro territorialmente competente, deve impartire una prescrizione, ai sensi dell'articolo 20 d.lgs n. 758/1994, al fine di porre rimedio all'irregolarità riscontrata mediante l'immediata cessazione della condotta illecita e la rimozione materiale degli impianti audiovisivi, essendo tale adempimento l'unico idoneo ad eliminare la contravvenzione accertata".*

SCHEMA TIPO DEL MANSIONARIO DEI TRATTAMENTI CARTACEI

Nel trattamento dei dati senza l'ausilio di strumenti elettronici (c.d. trattamenti su "carta") quando gli atti e i documenti contenenti dati personali 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. Tutta la documentazione contenente dati personali dovrà essere custodita in modo appropriato con modalità tali da impedire l'accesso a terzi non autorizzati.

SCHEMA TIPO DEL MANSIONARIO DEI TRATTAMENTI CON STRUMENTI ELETTRONICI

Per contribuire a garantire la sicurezza informatica dei trattamenti dei dati con strumenti elettronici, tutti i soggetti autorizzati al trattamento, sono tenuti al rispetto delle suddette prescrizioni sul corretto utilizzo degli strumenti elettronici e informatici (fotocopiatrici, stampanti, fax, telefono, computer, internet e posta elettronica, ecc.).

Si riportano le norme comportamentali da seguire.

- Si devono custodire gli strumenti elettronici ricevuti in dotazione in modo sicuro e corretto. Il dovere riguarda ogni tipologia di strumento ricevuto e quindi a titolo esemplificativo computer portatili, smartphone, tablet, periferiche di archiviazione di massa, ecc.;
- Si devono proteggere le proprie credenziali di autenticazione. La password non deve essere facilmente scopribile e deve essere periodicamente cambiata.
- È vietato partecipare a giochi online o giochi d'azzardo;
- È vietato utilizzare l'e-mail personale aziendale per finalità estranee all'attività lavorativa;
- Si devono utilizzare i servizi e le risorse informatiche dello studio/società come le e-mail o internet, principalmente e prevalentemente per scopi lavorativi;
- E vietato l'utilizzo dei propri dispositivi personali (quali telefoni cellulari, tablet, PC, Portatili, chiavette USB, etc.) per finalità lavorative senza previa autorizzazione del titolare;
- Si devono segnalare immediatamente eventuali incidenti informatici;
- È vietato utilizzare il proprio indirizzo personale di posta elettronica per distribuire informazioni riservate;
- È vietato lasciare incustoditi documenti aziendali, sulla scrivania, di natura riservata oppure dispositivi di archiviazione;
- Si devono restituire celermente al termine del rapporto lavorativo tutti gli strumenti elettronici (es. computer portatili, smartphone, tablet, ecc.) avuti in dotazione;

9. VIDEOSORVEGLIANZA

La legge 11 dicembre 2012, n. 220, riforma il Codice Civile in materia condominiale. Tra i nuovi articoli è stato introdotto il 1122 *ter* con il quale è stata fatta definitiva chiarezza sulla maggioranza prevista per poter deliberare sull'installazione di un impianto di videosorveglianza in condominio richiamando il 2° comma dell'articolo 1136 c.c.. Se il Presidente dell'assemblea condominiale si limita a verificare il quorum deliberativo, l'amministratore dovrà preoccuparsi degli aspetti privacy da far deliberare e verbalizzare, per poi procedere alla loro applicazione e rispetto. Se pur al momento della redazione del presente quaderno non è noto il decreto legislativo di armonizzazione tra il D. Lgs 196/2003 e il Regolamento UE 2016/679, è auspicabile che i provvedimenti emessi dal Garante in questi anni non perderanno di efficacia e, pertanto, rimarrà valido il Provvedimento prescrittivo dell'8 aprile 2010 in materia di videosorveglianza (doc. web n. 1712680). Un buon amministratore dovrà, oltre a procedere a reperire preventivi di ditte specializzate che garantiscano l'installazione di prodotti certificati, avere chiaro quali sono gli adempimenti obbligatori, per i quali è previsto un regime sanzionatorio e dare una serie di indicazione ai condomini. *In primis* dovrà chiarire alla compagine condominiale che la raccolta, la registrazione, la conservazione e in generale, l'utilizzo di immagini attraverso un sistema di videosorveglianza configura un trattamento di dati personali (art. 4, comma 1, lett. b C. P. - art. 4, par. 1 p. 2 GDPR) e che è lecito solo quando rispetta i principi fondamentali previsti quali liceità, finalità, necessità e proporzionalità. Pertanto, un impianto di registrazioni di immagini è soggetto alla normativa completa in termini di trattamento dati ed è ammesso se il fine è quello della tutela del patrimonio immobiliare e della sicurezza delle persone che vi risiedono. Non dovrà eccedere nell'uso e nel controllo. Ad esempio, è contraria al principio di necessità e di proporzionalità la telecamera che punta il suo occhio sull'uscio di una abitazione privata oltre che sull'androne o riprenda il marciapiede esterno allo stabile dove magari sono presenti dei locali commerciali. Le immagini dovranno essere raccolte e custodite, trattandosi di dati personali, applicando le misure di sicurezza adeguate in base al rischio e all'incidenza sui diritti e le libertà fondamentali degli individui. Pertanto il dvr dovrà essere custodito in luogo non accessibile a estranei e dovranno essere previste protezioni fisiche e logiche. Le immagini potranno essere visionate solo da soggetti incaricati, identificati e nominati e, solo per scopi ben definiti. Ad esempio, gli incaricati potranno accedere alle registrazioni solo in caso di illecito grave (danneggiamenti alle parti comuni, furti nelle abitazioni, violenze personali), dopo che è stata presentata denuncia del fatto alle autorità competenti e, su richiesta esplicita e sotto il controllo del responsabile del trattamento dati o del titolare. Potranno altresì accedere al dvr per controlli manutentivi se previsti da un apposito contratto con il quale vengono disciplinati i periodi e le modalità di accesso. Nuovamente, tra gli aspetti fondamentali ritorna l'informativa. Il cartello che generalmente viene apposto nelle vicinanze delle telecamere, fa parte in realtà dell'informativa, cosiddetta informativa breve, è obbligatoria, e deve rispettare alcune regole base:

- deve essere posto prima dell'angolo di ripresa delle telecamere;
- se l'impianto è funzionante anche di notte il cartello dovrà essere posto in un luogo illuminato;

- deve riportare indicazioni del titolare del trattamento delle immagini, il condomino, e le finalità, sicurezza delle persone e del patrimonio.

Accanto all'informativa breve, l'amministratore dovrà predisporre una informativa completa, accessibile e resa disponibile a tutti i residenti del condominio ma anche a chi è stato ripreso dalle telecamere seppur accidentalmente. Altro aspetto di fondamentale importanza è il tempo di conservazioni delle immagini. La norma prevede che le immagini possono essere conservate per 24/48 ore e massimo fino a 7 giorni. Le immagini possono essere tenute registrate per 24 ore e fino a 48 in caso di giorni festivi, ad esempio il sabato e la domenica. Possono essere mantenute fino a un massimo di 7 giorni, senza necessità di verifica preliminare al Garante, nel caso in cui questo risulti da un documento interno. È evidente che l'amministratore dovrà preoccuparsi di far deliberare anche questo aspetto, verbalizzando il tempo massimo di registrazioni delle immagini dopo il quale dovranno essere cancellate o sovra scritte. In mancanza di una apposita delibera in merito, l'amministratore dovrà tarare la registrazione sulle 24 ore.

VIDEOSORVEGLIANZA	
Articolo 1122 ter C.C.	Possibilità di installare un impianto di videosorveglianza con il quorum deliberativo previsto dal 2° comma art. 1136 C.C.
Titolare del trattamento	Condominio Via/Piazza …
Finalità del trattamento	Sicurezza del patrimonio e delle persone
Tempi di registrazione	Massimo 7 giorni
Informativa	Cartellonistica – Informativa completa da esibire a semplice richiesta
Misure di sicurezza	Fisiche e logiche
Nomina responsabili e incaricati	Nomina scritta dei responsabili e degli incaricati
Verifica periodica	Verifica almeno annualmente del funzionamento dell'impianto di registrazione, dei tempi, degli angoli di ripresa, della cartellonistica
Presenza di dipendente	Rispetto art. 4 Statuto dei lavoratori. Istanza preventiva presso Ispettorato del lavoro
Estrazione immagini	È possibile estrarre le immagini solo secondo le finalità e per fatti rilevanti (la sfera privata delle persone ha un peso importante e dovranno essere valutati gli eventi prima di estrarre le immagini). Occorre una denuncia presso le Autorità di giustizia

10. CODICI DI CONDOTTA – CERTIFICAZONI

Il legislatore europeo, attraverso l'articolo 40 del Regolamentato UE 2016/679, introduce la possibilità di elaborare codici di condotta con il fine di agevolare la corretta applicazione del regolamento.

Posso essere redatti diversi codici di condotta a seconda dei vari settori di trattamento e in base alle esigenze specifiche delle imprese.

Tutti coloro che rappresentano categorie di titolari del trattamento, quali ad esempio le associazioni, possono elaborare un codice di condotta con lo scopo di agevolare l'applicazione del regolamento da parte degli aderenti, una vera e propria guida declinata al singolo settore di appartenenza o tipologia di trattamento dei dati effettuato.

L'articolo 40 paragrafo 2 elenca, in modo esemplificativo e non esaustivo, quelle che potrebbero essere i contenuti di un codice di condotta.

Il vantaggio per gli aderenti al codice di condotta è avere uno strumento di applicazione del regolamento studiato verticalmente su quella data attività economica o categoria di titolari del trattamento.

Essendo gli amministratori di condominio una categoria tra le più numerose di professionisti con diverse associazioni di rappresentanza, è auspicabile che una o più associazioni aprano dei tavoli ove studiare e redigere un codice di condotta da sottoporre all'approvazione dell'Autorità di controllo.

CODICI DI CONDOTTA	
Istruzioni mirate per dare attuazione al GDPR per i trattamenti nel contesto specifico (ex amministrazioni e gestioni condominiali) **Interazione condivisa con l'Autorità di controllo**	Art. 40 par. 2 ...a esempio relativamente a: a) il trattamento corretto e trasparente dei dati; b) i legittimi interessi nel contesto specifico; c) la raccolta dei dati personali; d) la pseudonimizzazione dei dati personali; e) l'informazione fornita al pubblico e agli interessati; ... f) l'esercizio dei diritti degli interessati; g) l'informazione fornita e la protezione del minore; h) le misure tecniche e organizzative adeguate al rischio, la protezione dei dati fin dalla progettazione, le misure di sicurezza dei trattamenti; … l) la notifica di una violazione dei dati all'Autorità di controllo e, se del caso, la comunicazione i tali violazioni dei dati personali all'interessato; … j) il trasferimento dei dati personali verso paesi terzi; k) le procedure stragiudiziali e di altro tipo per comporre le controversie

Altrettanta importanza riveste la certificazione, vale a dire quella procedura trasparente attuata dall'Autorità di controllo o da un soggetto terzo accreditato che attraverso uno schema di certificazione riconosciuto dall'Autorità di controllo, certifica il rispetto del GDPR secondo detto schema.

L'adesione volontaria ai codici di condotta, così come l'ottenimento di una certificazione al trattamento dei dati effettuato da un titolare o responsabile al trattamento dei dati, non mette al riparo dai controlli che l'Autorità può eseguire.

TEST DI AUTOVALUTAZIONE

Un breve test di autovalutazione per avere una indicazione se i processi messi in atto presso lo studio/organizzazione sono diretti verso la conformità al GDPR.

Assegnare i seguenti punteggi alle risposte:

R.1 punteggio 2

R.2 punteggio 4

R.3 punteggio 7

R.4 punteggio 10

Un punteggio alto non è indice di conformità.

Se il risultato è compreso tra:

punteggio 80 – 100

lo studio/organizzazione è sulla rotta giusta. Proseguire nel processo di implementazione del sistema privacy facendo particolare attenzione alle misure tecniche e organizzative per garantire un buon standard di sicurezza e alle informative agli interessati;

punteggio 50 - 79

lo studio/organizzazione ha necessità di lavorare ancora per ottenere un adeguamento al GDPR soddisfacente;

punteggio 35 – 49

lo studio/organizzazione ha eseguito solo alcuni passi verso la conformità. Manca ancora molto lavoro;

punteggio meno di 35

non c'è più tempo. È urgente prendere in considerazione l'aiuto di un professionista per ridurre i tempi di adeguamento alla normativa

D. Nella sua organizzazione è stata eseguita una mappatura dei processi che coinvolgono l'uso di archivi non automatizzati?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione è stato dato incarico a una persona o si sta occupando personalmente dell'adeguamento dei processi e della modulistica secondo i dettami del GDPR?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione sono stati individuati tutti i trattamenti soggetti al GDPR?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione è stata eseguita una verifica della struttura informatica e sono stati analizzati i potenziali rischi?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione sono state formate e istruite le persone incaricate al trattamento dei dati?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione ha verificato se è nelle condizioni di dover eseguire una valutazione di impatto privacy?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione ha verificato se è stata fornita o resa disponibile l'informativa sul trattamento dei dati agli interessati e se questa contiene le informazioni previste dal GDPR?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione ha verificato se è necessario ottenere il consenso degli interessati rispetto alle finalità e ai trattamenti effettuati?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione ha predisposto una procedura per rispondere in tempi utili alle richieste che dovessero pervenire dagli interessati?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Sì, è una attività che ho iniziato a fare e sono a buon punto

D. Nella sua organizzazione ha verificato se sono tutelati i diritti degli interessati?

1. No, perché non mi sono posto il problema;
2. No, pur consapevole ritengo dare priorità ad altro;
3. No, ma ho interessato una persona a questa attività;
4. Si, è una attività che ho iniziato a fare e sono a buon punto

LA CERTEZZA DI UNA *"SOLUZIONE PRIVACY"* CERTA

Sei un amministratore di condominio o di complessi residenziali? Sei una azienda che si occupa di gestioni immobiliari? Hai uno studio professionale? Sai come gestire la privacy dei dati personali dei tuoi clienti?

Se raccogli e utilizzi dati anagrafici e altre informazioni dei tuoi clienti allora potremmo esserti di aiuto.

Il GDPR, il nuovo regolamento europeo sul trattamento dei dati personali, introduce nuovi obblighi per gli amministratori di condominio e più in generale chiunque raccoglie o gestisce dati personali di persone fisiche per la loro attività (imprenditori, liberi professionisti, PMI e grandi imprese).**L'Europa richiede alle aziende di essere a norma prima del 25 maggio 2018.** Noi possiamo aiutarti nel percorso di adeguamento richiesto dalla nuova normativa e a trasformare questo obbligo in nuove opportunità di business. Nel dare valore ai dati in tuo possesso, possiamo farti evitare o ridurre il rischio dell'incorrere nelle dure sanzioni previste dalle nuove norme e i connessi rischi amministrativi e penali.

Rokler Management & Consulting, nata dall'esperienza in ambito condominiale e immobiliare offre,oltre consulenza esperta privacy, l'integrazione dei processi interni all'azienda con un software completo per la gestione della protezione dei dati personali calibrato per l'amministratore condominiale e le aziende immobiliari: *"SOLUZIONE PRIVACY"*.

Adempi al nuovo regolamento europeo (GDPR), crei valore per la tua impresa e tuteli il tuo business. Affrettati, il tempo stringe!

Richiedi subito la consulenza Rokler e la DEMO GRATUITA di Soluzione Privacy, il software che semplifica la gestione della privacy.

www.soluzioneprivacy.com **codice promo CO-WEB2018BA**

Il software è disponibile online e non necessita di alcuna installazione

www.rokler.it **Via Albalonga, 16 - 00183 Roma – Tel: (+39) 06 89534942**

info@rokler.it **Via Monte Napoleone, 8 - 20121 Milano - Tel: (+39) 02 94420305**

facebook/@roklermc numero verde Help Privacy 800 035 194