

**REGOLAMENTO (UE)
2016/679 DEL PARLAMENTO
EUROPEO E DEL CONSIGLIO
del 27 aprile 2016**



Gdpr, Garante privacy: nessuna pronuncia su differimento applicazione sanzioni

Con riferimento a notizie circolanti in Internet è necessario precisare che non è vero che il Garante per la protezione dei dati si sia pronunciato sul differimento dello svolgimento delle funzioni ispettive e sanzionatorie né il provvedimento richiamato nei siti attiene a tale materia.

Nessun provvedimento del Garante, peraltro, potrebbe incidere sulla data di entrata in vigore del Regolamento europeo fissata al 25 maggio 2018.

Roma, 19 aprile 2018

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016

- Il regolamento è in se una rivoluzione, in quanto prende atto dello stato tecnologico ed espressamente si occupa dei dati informatici
- Andremo a vedere come questa nuovo regolamento si avvicini molto alla regolamentazione sulla sicurezza

RIVOLUZIONE CHE NON E' RIVOLUZIONE

Terminologia

«**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Terminologia

Condominio Sicuro

«**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

in Cloud

Terminologia

«**dato personale**»: 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;

Terminologia

Condominio Sicuro

in Cloud

«**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Terminologia

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

Condominio Sicuro
in Cloud

Ma in condominio si applica oppure no la normativa privacy?

Articolo 2

Ambito di applicazione materiale

1. Il presente regolamento si applica al **trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio** o destinati a figurarvi.
2. Il presente regolamento **non si applica** ai trattamenti di dati personali:
 - a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
 - b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
 - c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
 - d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Fondamenti di liceità del trattamento

- Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Quando posso trattare i dati?

Il trattamento è lecito solo se e nella misura in cui **ricorre almeno una** delle seguenti condizioni:

- a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- b) **il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;**
- c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

Quando posso trattare i dati?

- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Consenso - Novità rispetto alla 196/03

Per i dati "sensibili" (si veda art. 9 regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22). Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione. •

in Cloud

Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Consenso cosa non è cambiato rispetto alla 196/03

- Deve essere, in tutti i casi, libero, specifico, **informato** e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
- Deve essere manifestato attraverso “dichiarazione o azione positiva inequivocabile”

Amministratore di condominio ha bisogno del consenso?

- In generale si può affermare che **l'amministratore è comunque esonerato** (ex art. 24 del codice della privacy) dalla necessità del consenso da parte dei singoli condomini al trattamento dei dati dovendo adempiere un obbligo previsto dalla legge (cfr. artt. 1130 ss. c.c.).
- Più specificamente si deve evidenziare che il Garante è intervenuto in materia condominiale con il provvedimento «Amministrazione dei condomini» del 18 maggio 2006 (pubblicato sulla Gazzetta Ufficiale n. 152 del 3 luglio 2006) in cui ha precisato i compiti dell'amministratore in relazione al trattamento delle informazioni inerenti la gestione e l'amministrazione delle parti comuni.
- Tali informazioni possono riguardare **sia tutto il condominio (es. dati relativi ai consumi) sia i singoli partecipanti (dati anagrafici, catastali, quote millesimali, ecc.)**.

Attenzione

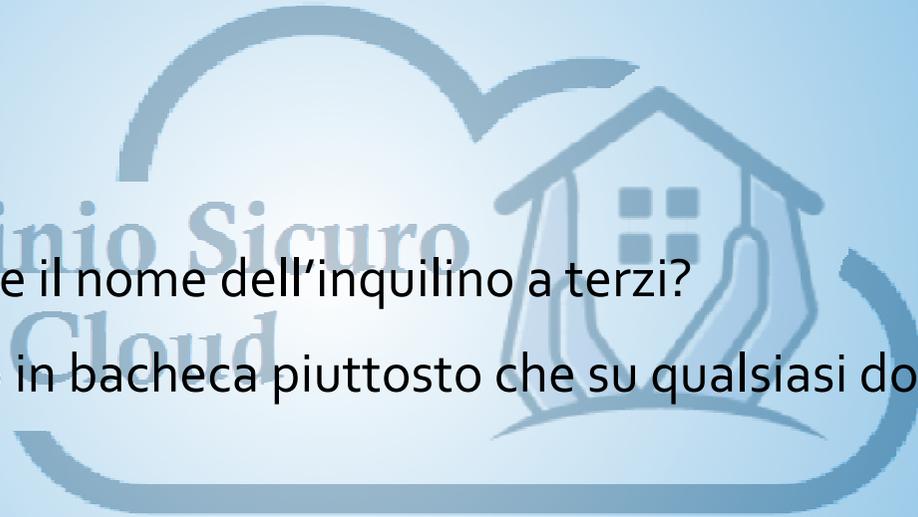
L'USO DI NON TUTTI I DATI CHE RACCOGLIAMO QUOTIDIANAMENTE SONO ESENTI DAL CONSENSO

- In particolare i dati sono trattabili solo se indispensabili ai fini dell'amministrazione del condominio.
- Il provvedimento del garante ha quindi stabilito quali dati possono essere trattati senza il consenso dell'interessato (es. «*le informazioni personali pertinenti e necessarie rispetto allo svolgimento delle attività di gestione ed amministrazione*» del condominio) e quali invece **richiedono il suo specifico consenso** per poter essere trattati dall'amministratore del condominio (es. «*informazioni relative alle utenze telefoniche intestate ai singoli partecipanti*»).

Facciamo degli esempi

- E' possibile comunicare il nome dell'inquilino a terzi?
(mettendolo ad esempio in bacheca piuttosto che su qualsiasi documento
esempio rendiconto?)

Condominio Sicuro
in Cloud



NO!

- **Contratti di locazione: vietata la diffusione a terzi dei dati personali del conduttore - 20 novembre 2008 [1576139]**

[...] VISTA la segnalazione del 18 gennaio 2008, con cui XY, in qualità di conduttore di una stanza di un appartamento di proprietà di un condominio sito in Taranto, lamenta l'avvenuta diffusione di dati personali a sé riferiti (nel dettaglio, la notizia relativa alla scadenza prossima del contratto di locazione in essere tra il segnalante ed il medesimo condominio, stabilita per il mese di gennaio 2009, e la contestuale intimazione al rilascio dell'immobile alla citata scadenza) da parte della stessa compagine condominiale, ancorché per il tramite dell'amministratore *pro-tempore*;

[...] TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice, dispone nei confronti del condominio di Via KZ n. 3 (nella persona dell'amministratore *pro-tempore*), **il divieto dell'ulteriore diffusione in bacheca o altro luogo nel quale sia visibile** da chiunque dei dati personali riferiti, anche indirettamente, al segnalante e relativi alla scadenza del contratto di locazione in essere tra il medesimo segnalante e il condominio, con effetto dalla data di ricezione del presente provvedimento.

Come si risolve in Geco?

Entro nella scheda anagrafica del condòmino e in "note/contatto" inserisco dicitura, es. inquilino. Quest'ultima sarà la dicitura visionata nelle varie stampe.



	Mil
EDIFICIO	
SCALA	
1 - (PR) Paolini Mariella	100,00
2 - (PR) Chiansi Saverio	170,00
2 - (IN) Inquilino	0,00
3 - (PR) Mausè Giuseppina	300,00
4 - (PR) Mascheri Renzo	350,00
Totale SCALA	920,00
BOX	
1 - (PR) Paolini Mariella	20,00
1 - (IN) Inquilino	0,00
2 - (PR) Paolini Mariella	20,00
3 - (PR) Masci Lorenza	20,00
4 - (PR) Mascheri Renzo	20,00
Totale BOX	80,00
Totale EDIFICIO	1.000,00

In Particolare

- Si ha l'obbligo di gestire i contatti con l'inquilino in virtù del concetto di bene comune MA non si possono comunicare a terzi, SALVO SPECIFICI CASI.
- Come in realtà non è possibile comunicare a nessun terzo i dati dei singoli condomini (salvo quelli necessari a svolgere la propria mansione)

Comunicazione dati TUTELATI a Terzi in caso di emergenza

Provvedimento del 13 dicembre 2012 [2337896]

VISTO il ricorso, regolarizzato il 1° agosto 2012, con il quale XY ha ribadito, nei confronti del Sig. Nicola Schina, in qualità di amministratore del condominio nel quale risiede, l'opposizione al trattamento dei dati relativi al proprio **numero di telefono portatile** che sarebbe stato oggetto di successiva comunicazione, da parte del citato amministratore, ad un'impresa (Focus s.r.l.) incaricata di alcuni lavori condominiali; visto che l'interessata, nel precisare che il predetto numero di telefono era stato comunicato "all'amministratore solo per comunicazioni che avvengono (...) tra la sottoscritta e l'Amministratore", ha anche chiesto di porre a carico di controparte le spese del procedimento;

Comunicazione dati TUTELATI a Terzi in caso di emergenza

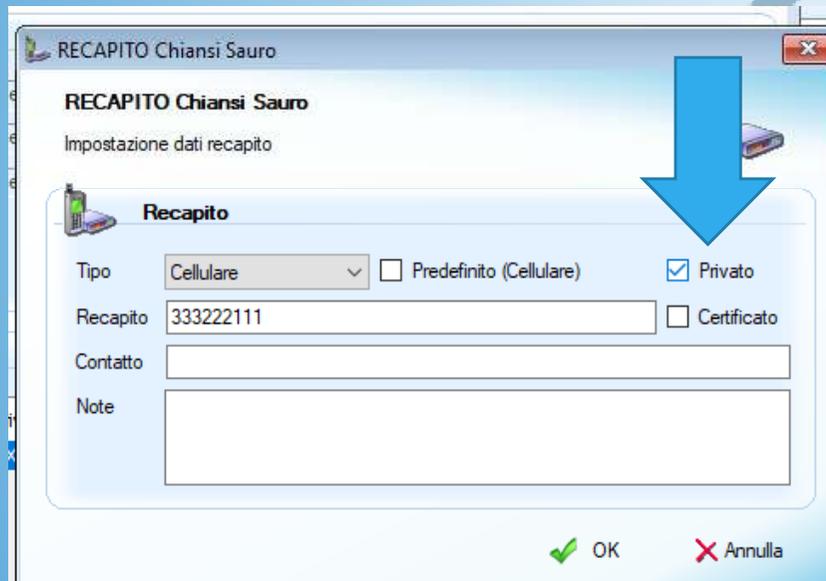
- VISTA la nota del 3 settembre 2012 con la quale il titolare del trattamento ha precisato che l'utilizzo dei dati dei condòmini è necessario per il concreto svolgimento dell'attività di amministratore e che, in particolare, i recapiti telefonici dell'interessata "erano in mio possesso in quanto a me forniti dall'amministratore precedente (...)"; visto che la contestata comunicazione dei dati alla società Focus s.r.l. sarebbe avvenuta "**per esigenze pratiche di urgenza e necessità in quanto l'assemblea dei condòmini aveva deliberato (...) la manutenzione ordinaria delle porte antincendio ubicate presso lo stabile condominiale**"; visto che l'amministratore ha anche precisato che due condòmini (tra cui la Sig.a XY) in occasione di tale assemblea gli avevano consegnato alcuni preventivi (fra cui quello proposto dalla citata Focus s.r.l.) raccomandandosi di procedere con urgenza ai lavori di riparazione; visto che l'amministratore, nel precisare che "la ditta Focus ha tentato di chiamare solo due volte la signora XY", ha sostenuto di aver già eliminato l'utenza telefonica dell'interessata dai suoi contatti, iniziativa già adottata anche dalla società Focus;

Comunicazione dati TUTELATI a Terzi in caso di emergenza

- VISTE le memorie del resistente datate 3 ottobre e 22 novembre 2012 nelle quali l'amministratore ha fornito ulteriori particolari atti a ricostruire la vicenda in questione, specie con riguardo all'equivoco che ha indotto il resistente a ritenere che la ricorrente fosse una delle referenti della società Focus all'interno del condominio, **attesta anche la necessità di avere accesso al fabbricato interessato dagli urgenti lavori di riparazione (costruzione di cui l'amministratore non detiene le chiavi);**
- RITENUTO **di dover dichiarare non luogo a provvedere** sul ricorso avendo il resistente fornito un adeguato riscontro alle richieste dell'interessata, sia pure solo nel corso del procedimento;

Come si risolve in Geco?

Rendo privato il recapito, mettendo il flag



RECAPITO Chiansi Sauro

RECAPITO Chiansi Sauro

Impostazione dati recapito

Recapito

Tipo Predefinito (Cellulare) Privato

Recapito Certificato

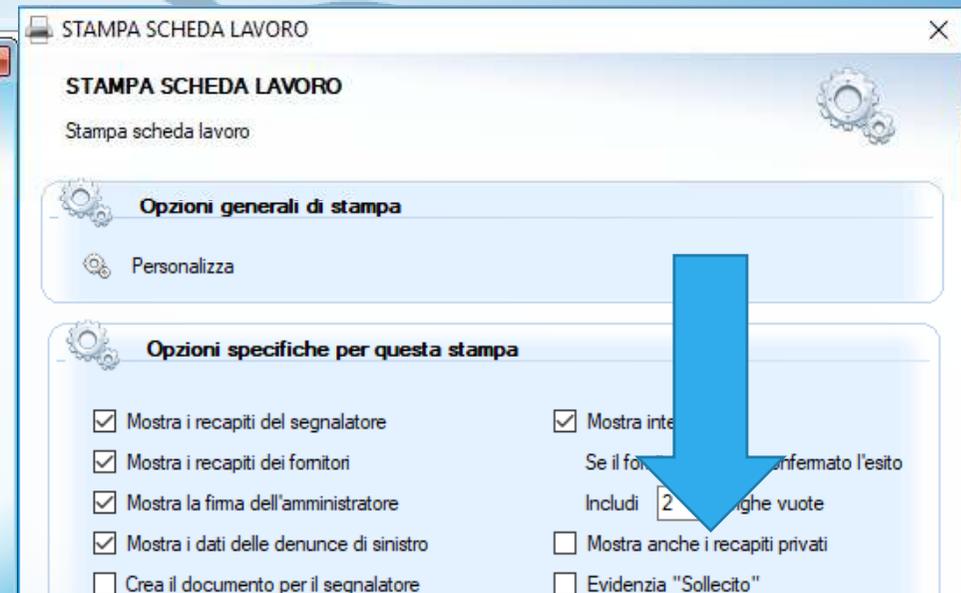
Contatto

Note

OK Annulla

Recapiti dei condomini

Nel momento in cui andrò a stampare una scheda lavoro, dovrò ricordarmi di inserire il flag su "mostra anche i recapiti privati"



STAMPA SCHEDA LAVORO

Stampa scheda lavoro

Opzioni generali di stampa

Personalizza

Opzioni specifiche per questa stampa

Mostra i recapiti del segnalatore Mostra inter...

Mostra i recapiti dei fornitori Se il for... confermato l'esito

Mostra la firma dell'amministratore Includi 2 righe vuote

Mostra i dati delle denunce di sinistro Mostra anche i recapiti privati

Crea il documento per il segnalatore Evidenzia "Sollecito"

Apertura Scheda Lavoro

Curiosità

Capiamo perché la normativa spesso non viene considerata in ambito condominiale

- Quanti tra i presenti quotidianamente hanno compiuto atti simili a quelli qui riportati?
- Perché nessuno dei presenti ha subito una sanzione?
- Chi è il soggetto che deve denunciare l'amministratore in caso di violazione della privacy?

Condominio Sicuro
in Cloud



Circolo Vizioso - Virtuoso



In altre parole

Nel momento in cui avrò un condomino scontento, che sarà a conoscenza dei propri diritti, esso avrà un ulteriore campo in cui, se non ci mettiamo in linea, farci sanzionare.

Per meglio spiegare questo concetto, anche se anticipiamo l'obbligo dell'informativa voglio mostrare una sentenza fortunatamente vinta da un vostro collega.

Provvedimento del 5 dicembre 2013

[2951902]

[...]VISTO il ricorso, presentato in data 16 luglio 2013 nei confronti di XY, in qualità di amministratore del "Condominio JJ", **con cui KW e HJ**, comproprietari di un immobile facente parte del predetto condominio, nel ribadire le istanze già avanzate ai sensi degli artt. 7 e 8 del Codice in materia di protezione dei dati personali (di seguito "Codice"), hanno chiesto, oltre ad alcune richieste non riconducibili all'esercizio dei diritti di cui ai predetti articoli, di conoscere l'origine dei dati personali che li riguardano, **la comunicazione delle finalità, delle modalità e della logica applicata al trattamento, gli estremi identificativi del titolare del trattamento, del soggetto eventualmente nominato responsabile del trattamento**, nonché dei soggetti incaricati, chiedendo altresì la cessazione del trattamento in ordine ad alcune operazioni di cui gli interessati hanno lamentato l'illegittimità. Ciò con riferimento specifico alla **"confusione di ruoli e responsabilità tra l'amministratore nominato dall'assemblea (il sig. XY), altri soggetti allo stesso collegati (con particolare riferimento al sig. XY) e, più genericamente, lo Studio professionale riconducibile ai medesimi soggetti (...)"** (soggetti cui peraltro gli interessati hanno inviato anche il previo interpello), i quali, pur in assenza di un esplicito consenso espresso dai ricorrenti, avrebbero "diffusa facoltà di accesso" ai dati personali riferiti agli stessi; i ricorrenti hanno chiesto altresì la liquidazione in proprio favore delle spese sostenute per il procedimento; [...]

Ricapitoliamo: **FONDAMENTI DI LICEITA'** **DEL TRATTAMENTO**

- Amministratore di Condominio HA SEMPRE diritto di trattare (NON COMUNICARE) i dati degli amministrati, SENZA AVERE NESSUN consenso scritto, purché essi siano i minimi necessari per adempiere al suo mandato.
- In caso di **COMPROVATA** emergenza può utilizzarli e comunicare a terzi **SENZA NESSUN CONSENSO**
- Il **CONSENSO** può essere di tipo informatico

Ribadiamo ma tutti i dati?

L'Autorità ha ribadito innanzitutto che, in base alla disciplina privacy, l'amministratore può trattare solo informazioni pertinenti e non eccedenti rispetto alle finalità da perseguire. **Può**, dunque, acquisire le informazioni che consentono di identificare e contattare i singoli partecipanti al condominio - siano essi proprietari, usufruttuari, conduttori o comodatari - chiedendo le generalità comprensive di codice fiscale, residenza o domicilio. Può chiedere, inoltre, i dati catastali: la sezione urbana, il foglio, la particella, il subalterno e il Comune.

Non può invece chiedere, perché risulterebbe eccedente, copia della documentazione: come, ad esempio, l'atto di compravendita in cui sono riportati i dati. Per quanto riguarda poi le informazioni relative alle "condizioni di sicurezza", con l'entrata in vigore del "Decreto Destinazione Italia" i condòmini non dovranno più fornire alcuna informazione sulla propria unità immobiliare, perché i dati da raccogliere riguardano solo le parti comuni dell'edificio.

Grosso cambiamento!

Condominio Sicuro
in Cloud

Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **NON SPETTA** all'Autorità ma **è compito dello stesso titolare**; si tratta di una delle principali espressioni del principio di «responsabilizzazione» introdotto dal nuovo pacchetto protezione dati.

Informativa... Questa sconosciuta!

Informativa era un obbligo, e lo rimane anche oggi....

Condominio Sicuro
in Cloud

Ovviamente ha subito delle modifiche formali

Cosa non è cambiato?

L'informativa (*disciplinata nello specifico dagli artt. 13 e 14 del regolamento*) deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento).

Se i dati non sono raccolti direttamente presso l'interessato (*art. 14 del regolamento*), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

- **NOTA:** ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Cosa Cambia? **Contenuti dell'informativa**

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **DEVE SEMPRE** specificare i **dati di contatto del [RPD-DPO](#)** (Responsabile della protezione dei dati-Data Protection Officer), ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti**

Cosa Cambia? **Contenuti dell'informativa**

Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente":

in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.

Ma la Frequenza?

Non è stata indicata, salvo essere congrua al fine che l'interessato abbia conoscenza dei suoi diritti.

Annuale? **O meglio Sempre disponibile?**

Dopotutto come vedremo viene indicato la preferenza di un sistema informatico

Tempi dell'informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato)

(diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee (*si veda anche considerando 58*).

Modalità dell'informativa

L'informativa è data, in linea di principio, per iscritto e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Esonero dell'informativa

Sono inoltre parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), **anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

Esonero dell'informativa: Non rientra amministratore di condominio

I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) **l'interessato dispone già delle informazioni;**

b) **comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;** in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) **l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato;**

d) qualora i dati personali debbano rimanere riservati conformemente **a un obbligo di segreto professionale** disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge

Ordinanza di ingiunzione nei confronti del dott. Luigi Ventrone - 19 settembre 2013

[...] RILEVATO che, a seguito di una segnalazione pervenuta in data 28 luglio 2010 da parte della sig.ra Ilaria Corsale con cui veniva lamentato un comportamento illecito tenuto nei suoi confronti da parte del dott. Luigi Ventrone, amministratore pro tempore del condominio "Palazzo Noviello", sito in via Roberto d'Angiò, Santa Maria Capua Vetere (CE), il Dipartimento realtà economiche e produttive formulava una richiesta di informazioni al dott. Ventrone, datata 20 maggio 2011 (prot. n. 10620/70114), diretta a ottenere ogni informazione utile alla valutazione del caso, **con particolare riferimento alle modalità e alle finalità del trattamento dei dati** relativi alla sig.ra Corsale; [...]

Ordinanza di ingiunzione nei confronti del dott. Luigi Ventrone - 19 settembre 2013

[...] VISTO lo scritto difensivo inviato ai sensi dell'art. 18 della legge 24 novembre 1981 n. 689, con cui il dott. Ventrone ha dichiarato che, a causa dei propri impegni lavorativi, non ha potuto provvedere a fornire i chiarimenti richiesti e di aver consegnato tutta la documentazione relativa alla vicenda al proprio legale, confidando che questi vi provvedesse. Ha, inoltre, precisato di non sapere "dell'esistenza di un preciso obbligo giuridico relativo alla richiesta trasmissione di informazioni, ritenendo tale adempimento una mera facoltà (...)"; [...]

Ordinanza di ingiunzione nei confronti del dott. Luigi Ventrone - 19 settembre 2013

ORDINA

al dott. Luigi Ventrone, nato a Santa Maria Capua Vetere (CE) il 29 aprile 1967, nella sua qualità di amministratore pro tempore del Condominio "Palazzo Noviello" sito in via Roberto d'Angiò, Santa Maria Capua Vetere (CE), di pagare la somma di euro **4.000,00 (quattromila)** a titolo di sanzione amministrativa pecuniaria per la violazione prevista dall'art. 164 del Codice indicata in motivazione;

Geco:

Scheda anagrafica condominio-Privacy-Inserire testo informativa privacy per stampe-indicare il responsabile del trattamento e, se presenti, altri eventuali responsabili

Condominio EMILIA

Condominio

- Salva
- Salva & Chiudi
- Annulla

Strumenti

- Crea scheda
- Verifica privacy

Stampe

Condominio EMILIA

Impostazioni dati condominio

Dati Conti Num. utili Contatori/polizze Privacy Fiscali Studi di settore Ascensori / Varie Allegati

Dipendenti

Nominativo	Dal	Al

Nuovo Dettagli Elimina Sposta su Sposta giù

Privacy

Testo informativa privacy per le stampe

Per consultare l'Informativa privacy recarsi sul sito www.condominiosicuro.info/privacy-online muniti di codice fiscale del condominio

Responsabile trattamento **X** [GECO2010](#)

Altri responsabili trattamento dati	Note

Nuovo Dettagli Elimina Applica impostazioni Sposta su Sposta giù

DATI LICENZA 

Impostazione dati licenza d'uso

 Dati licenza  Amministratori

 **Amministratori**

Nominativo
Studio Demo
GECO2010

 Nuovo  Dettagli  Elimina  Sposta su  Sposta giù

 **Dati di stampa**

Testo informativa privacy per le stampe

Intestazione

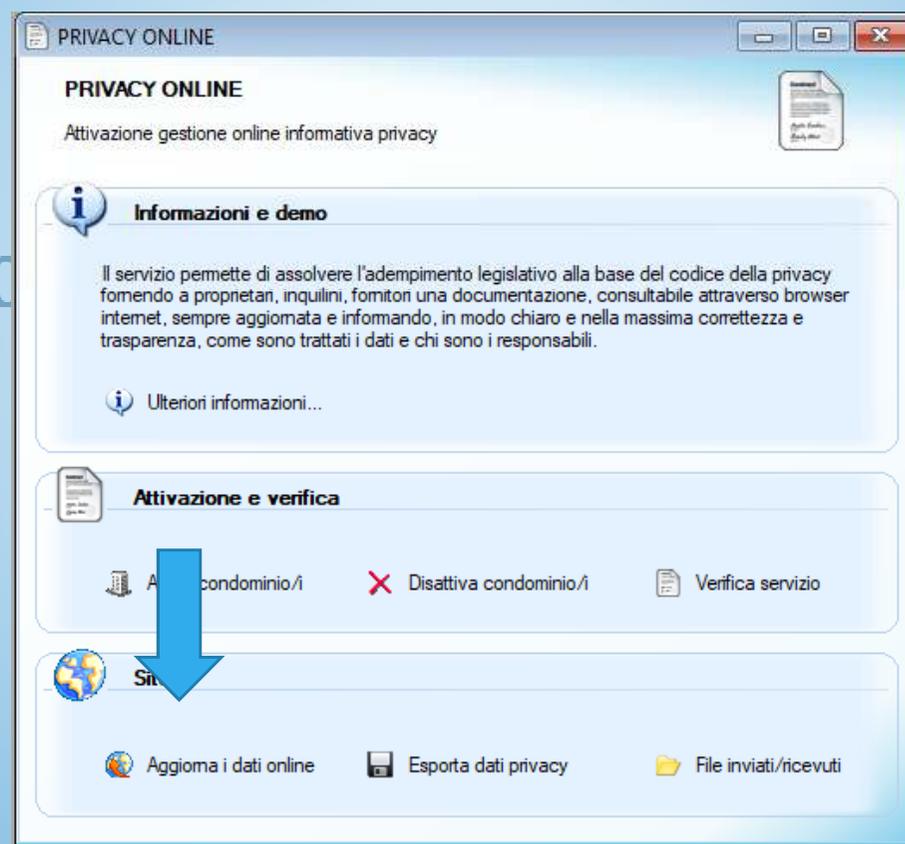
Nei dati dell'intestazione includi anche il luogo di stampa

Piè di pagina

Nei dati licenza, ho la possibilità di scegliere la posizione in cui visionare il testo dell'informativa (intestazione o piè di pagina)



Come ultima procedura bisogna aggiornare i dati online



Ordinanza di ingiunzione nei confronti di Vincenzo Cipriani - 2 luglio 2015

RILEVATO che, a seguito di una segnalazione pervenuta in data 26 novembre 2010 con la quale l'interessato lamentava un comportamento illecito nei suoi confronti da parte del sig. **Vincenzo Cipriani, in qualità di amministratore del condominio di via Asti n. 5 di Terlizzi (Ba)**, il Dipartimento realtà economiche e produttive inviava una richiesta di informazioni datata 18 maggio 2011, con la quale si invitava il citato soggetto a fornire ogni elemento e informazione utile alla valutazione del caso, alla quale non veniva data alcuna risposta;

Ordinanza di ingiunzione nei confronti di Vincenzo Cipriani - 2 luglio 2015

RITENUTO, ad ogni buon conto, che quanto dedotto nella citata opposizione non risulta idoneo in relazione a quanto contestato. Del tutto arbitrariamente il trasgressore ha fissato al 15 giugno 2011 la data dell'accertamento della violazione relativa all'omessa informazione o esibizione al Garante (art. 164 del Codice), che deve invece riferirsi al 19 agosto 2011. Dall'esame della documentazione agli atti, emerge che il termine indicato dall'Ufficio per la trasmissione all'Autorità dei documenti e delle informazioni richieste ex art. 157 del Codice, era il 19 agosto 2011 e che pertanto, allo spirare del citato termine deve essere ricondotto il dies a quo previsto dall'art. 13 della legge n. 689/1981, per la notificazione del verbale di contestazione. Nel caso di specie la notifica, effettuata il 3 novembre 2011, è avvenuta nel pieno rispetto del termine di 90 giorni dall'accertamento della violazione richiesto a pena di decadenza dalla norma;

Ordinanza di ingiunzione nei confronti di Vincenzo Cipriani - 2 luglio 2015

ORDINA

al sig. Vincenzo Cipriani quale amministratore pro-tempore del condominio di via Asti n. 5 Terlizzi (Ba), di pagare la somma di euro **4.000,00 (quattromila)** a titolo di sanzione amministrativa pecuniaria per la violazione prevista dall'art. 164 del Codice;

Informativa: ricapitoliamo

- Invio informativa: obbligatoria ed entro e non oltre un mese dal verbale di acquisizione del condominio
- Modalità: preferire forme informatiche in modo tale da essere facilmente reperibile
- Deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**

Modalità per l'esercizio dei diritti (cosa non è cambiato)

- **Il titolare del trattamento deve agevolare l'esercizio dei diritti** da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo titolare a dover dare riscontro** in caso di esercizio dei diritti (*artt. 15-22*), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (*art. 28, paragrafo 3, lettera e*).

Modalità per l'esercizio dei diritti (cosa non è cambiato)

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni

Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

Modalità per l'esercizio dei diritti (cosa non è cambiato)

Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).

Cosa invece è cambiato?

Condominio Sicuro
in Cloud

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Cosa invece è cambiato?

Spetta al titolare valutare **la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato**, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12.5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.

Cosa invece è cambiato?

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

Cosa invece è cambiato?

Condominio Sicuro

In Cloud

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Diritto di accesso (art. 15)

- Il diritto di accesso prevede in ogni caso il **diritto di ricevere una copia dei dati personali** oggetto di trattamento.
- Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, **mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo**, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Diritto di cancellazione (diritto all'oblio) (art.17)

Il diritto cosiddetto **"all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata**. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).

Diritto di limitazione del trattamento (art. 18)

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, **tutela diritti di altra persona fisica o giuridica**, interesse pubblico rilevante).

Diritto alla portabilità dei dati (art. 20)

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al titolare (*si veda il considerando 68 per maggiori dettagli*).

Inoltre, il titolare deve essere in grado **di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato**, se tecnicamente possibile.

Nota: Conto Corrente

L'Autorità ha fornito ulteriori chiarimenti in merito al cosiddetto "conto condominiale", che deve essere aperto e utilizzato dall'amministratore, e sul diritto di ciascun condomino di accedere alla relativa documentazione. In particolare, a seguito della riforma, il Garante ha chiarito che nonostante il conto sia intestato al condominio **i singoli condòmini sono ora titolari di una posizione giuridica che consente loro di verificare la destinazione dei propri esborsi e l'operato dell'amministratore mediante l'accesso in forma integrale, per il tramite dell'amministratore, ai relativi estratti conto bancari o postali.**

Tale principio, già sancito in linea generale dal Garante nelle [Linee guida in ambito bancario \[doc. web n. 1457247\]](#), riconosce infatti il **diritto di ottenere "copia di atti o documenti bancari" senza alcuna limitazione, neanche nelle forme di un parziale oscuramento, anche se contengono dati personali di terzi.**

Attenzione ai tempi di risposta!!

Condominio Sicuro

in Cloud

- E se pensate che non capiti che vi venga richiesto la verifica da parte del garante a seguito di una segnalazione di un «presunto» illecito da parte di un condomino....



Provvedimento del 21 settembre 2017

[7421901]

VISTO il ricorso presentato al Garante in data 6 maggio 2017 da XX nei confronti della TG Tecnogestioni snc di Bettini Sandro e Milini Paolo, con il quale il ricorrente, ribadendo le istanze già avanzate, in data 7 maggio 2016 e 15 gennaio 2017, ai sensi degli artt. 7 e 8 del d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (di seguito, "Codice"), ha chiesto di ottenere:

1. la conferma dell'esistenza o meno dei dati personali che lo riguardano, anche se non ancora registrati e la loro comunicazione in forma intelligibile;
2. l'origine di tali dati, nonché le finalità, le modalità e la logica applicata al loro trattamento;
3. gli estremi identificativi del titolare e del responsabile;

Provvedimento del 21 settembre 2017

[7421901]

4. informazioni circa i soggetti o le categorie di soggetti ai quali i suoi dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e di rappresentante designato nel territorio dello Stato;

5. la cancellazione dei dati trattati in violazione di legge, compresi quelli scambiati a mezzo mail presenti sulla casella postale della resistente e conservati su qualsiasi supporto cartaceo e digitale;

6. l'accoglimento dell'opposizione al trattamento dei propri dati per i quali non è necessaria la conservazione;

il ricorrente ha, altresì, chiesto la liquidazione in proprio favore delle spese sostenute per il presente procedimento;

Provvedimento del 21 settembre 2017

[7421901]

VISTA la nota del 25 maggio 2017 con la quale la resistente, con specifico riferimento alle richieste avanzate dal ricorrente, ha rappresentato:

che i dati personali sono stati forniti attraverso la compilazione del modulo di acquisizione inserito nel Registro dell'anagrafe condominiale dallo stesso ricorrente, oppure trasmessi da quest'ultimo "in un'ottica di estrema collaborazione connaturata alla mansione di consigliere e all'ottimo rapporto che sussisteva con l'amministratore";

di non essere più in possesso dei dati contenuti in tale Registro, in quanto lo stesso è stato consegnato al nuovo amministratore del condominio;

Provvedimento del 21 settembre 2017

[7421901]

che le finalità del trattamento riguardavano lo svolgimento della gestione condominiale avvenuta attraverso modalità cartacee e informatiche;

di non avere nominato responsabili del trattamento, né di avere comunicato a terzi i dati del ricorrente;

la resistente ha, altresì, precisato di avere provveduto, come già comunicato al ricorrente con e-mail del 25 maggio 2016, "a cancellare il contatto dalla rubrica mail nonché il link alle comunicazioni contenute in eventuali cartelle condivise, oltre ai recapiti cellulari e telefonici";

Provvedimento del 21 settembre 2017

[7421901]

TUTTO CIÒ PREMESSO IL GARANTE:

- a) dichiara il ricorso inammissibile in ordine alla richiesta di cancellazione dei dati detenuti dalla resistente;
- b) dichiara non luogo a provvedere in ordine alle ulteriori richieste avanzate dal ricorrente ai sensi dell'art. 7 del Codice;
- c) determina l'ammontare delle spese del presente procedimento nella misura forfettaria di euro 500,00, di cui euro 200,00 da addebitarsi a TG Tecnogestioni snc di Bettini Sandro e Milini Paolo che dovrà liquidarli direttamente a favore del ricorrente; compensa la restante parte per giusti motivi.

Principale Novità!

- **APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI**

Non esistono più delle procedure minime standard MA CIASCUNO DEVE FARE UN'ANALISI DEI PROPRI RISCHI

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento).

Si tratta di una grande novità per la protezione dei dati in **quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali** – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY

Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY

- Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

Esempio

- Quali sono i rischi di «violazione dei dati personali» per amministratore di condominio?

la distruzione, la perdita, la modifica dei dati sono una violazione

- Come Evito questo?

Stabilisco una procedura DIMOSTRABILE di Backup del sistema!

Geco permette di fare un backup dati

The image shows the Geco software interface with the 'Database' menu open. The 'Backup e ripristino' sub-menu is selected, and the 'Backup dati' option is highlighted. A blue arrow points from this option to the 'BACKUP' dialog box on the right. The dialog box is titled 'BACKUP' and contains the following sections:

- Informazioni sull'archivio attuale:**
 - Archivio: arscd_belluno su 192.168.254.210
 - Versione 2.10.4.0
 - Testo di controllo file di backup (vecchio formato):
 - Testo iniziale: - PostgreSQL database dump 0.4
 - Testo finale: - PostgreSQL database dump complete 0.4
- Impostazioni backup archivio:**
 - Percorso utility con cui effettuare il backup: C:\Program Files (x86)\PostgreSQL\8.4\bin\pg_dump.exe
 - Esporta nel nuovo formato "Postgres" Compensi il file esportato
 - Backup su disco:**
 - Backup remoto:** Il servizio "Backup Remoto" permette di inviare una copia dei dati sul server di GeCo2010. In caso di necessità sarà possibile collegarsi al sito backup.geco2010.it ed effettuare il ripristino dell'archivio.
 - Collegati al sito Lista archivi sul sito
- Dettaglio comando:** (empty field)

The dialog box has a 'OK' button at the bottom right.

E la nostra T-Box

Offre un Backup giornaliero di geoco e dello studio; una protezione contro i malware che criptano i dati ed un Accesso protetto ai dati tramite combinazione utente e password .



Esempio

- Quali sono i rischi di «violazione dei dati personali» per amministratore di condominio?

la divulgazione non autorizzata dei dati sono una violazione

- Come Evito questo?

Stabilisco di avere un antivirus e un firewall aggiornato!

T-Box

- Offre un sistema centralizzato ed automatizzato per la protezione del traffico dati rilevando e bloccando eventuali malware (funzione antivirus), ovvero consente o nega gli accessi in virtù di regole statiche e dinamiche.



Dal legale all'informatico

- Se abbiamo visto in precedenza che era sufficiente avere dei bei moduli ben compilati la nuova normativa ci chiede di avere una tracciabilità del sistema informatico e di investire in esso.
- La privacy non è più ambito solo di legali ma diventa sempre più un sistema legato ad informatici

Responsabile della protezione dei dati

Condominio Sicuro
In Cloud

- Nasce infatti una nuova figura!!!
- Ancora troppo nebulosa... e soprattutto non prevista per tutta una serie di categorie



Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato

2. Quali requisiti deve possedere il responsabile della protezione dei dati personali?

Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.

Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").

In ogni caso, resta comunque raccomandata, anche alla luce del principio di ["accountability"](#) che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

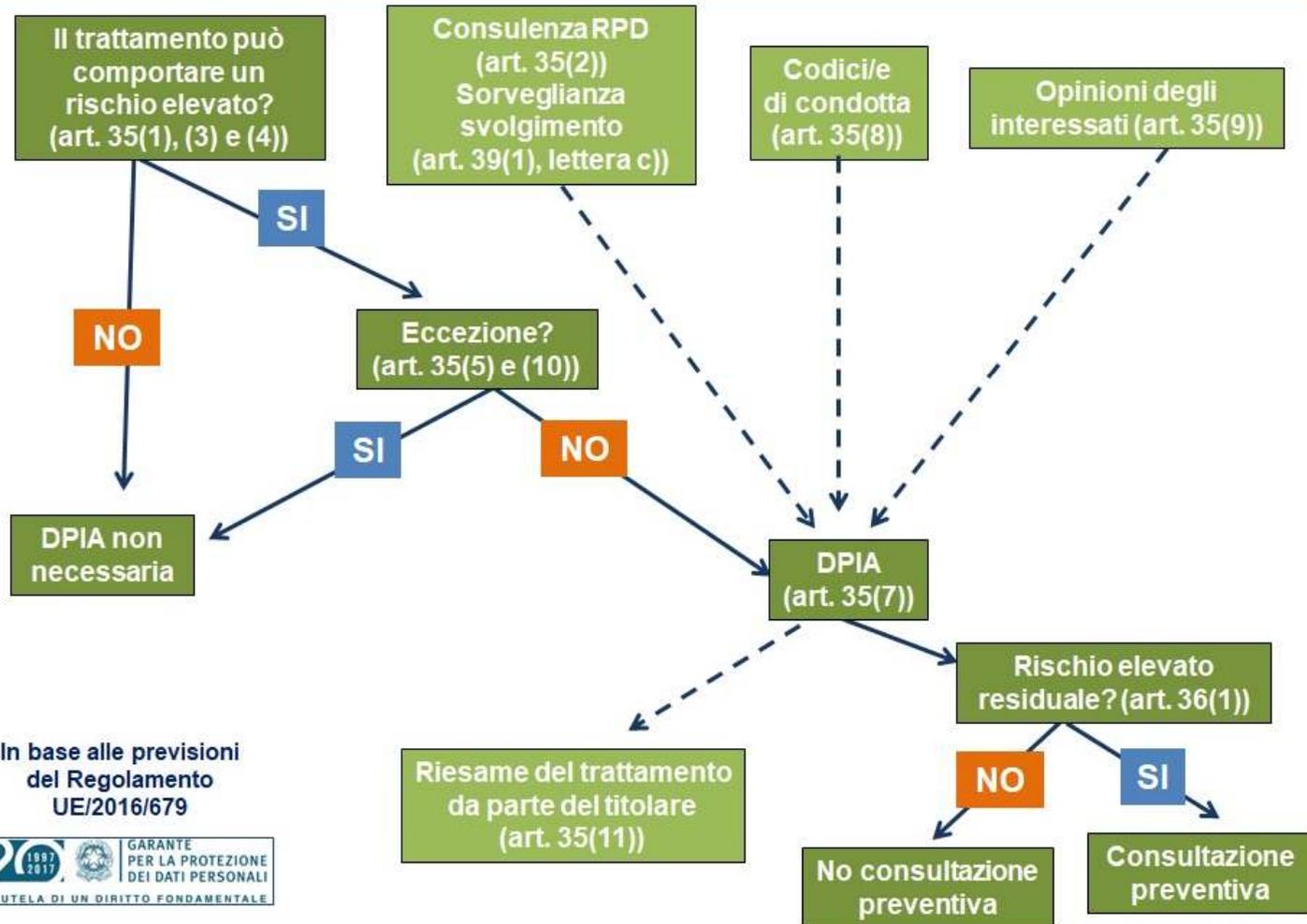
DPIA

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (*si vedano considerando 75-77*); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (*si vedano artt. 35-36*) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/DPIA).

All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla?



Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'articolo 35 del Regolamento UE/2016/679 (RGDP) che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento lo prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta prima di procedere al trattamento. Dovrebbe comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari.

CHI?

La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare ne monitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e accusando - se i trattamenti lo richiedono - il parere di esperti di settore, del responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer, CSO) e del responsabile IT.

QUANDO LA DPIA È OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:

- trattamenti valutativi o di scoring, compresa la profilazione;
 - decisioni automatizzate che producano significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipuli di assicurazioni);
 - monitoraggio sistematico (es: videosorveglianza);
 - trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
 - trattamenti di dati personali su larga scala;
 - combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari differenti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
 - dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
 - utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
 - trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).
- La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON È OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON** è necessaria per i trattamenti che:

- non presentano rischio elevato per i diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti UE o di uno stato membro, per la cui definizione è stata condotta una DPIA.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679

A pagina 13 riporta elenco di esempi per esemplificare chi è soggetto a fare il DPIA cita:

Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).

- Dati sensibili o dati aventi carattere estremamente personale.
- Dati riguardanti soggetti interessati vulnerabili.

Non È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati.

Farla o non Farla?

Condominio Sicuro in Cloud

- UNI10801: DVR / Verifiche elettriche Documento non cogente necessario per la corretta gestione



novi criteri per stabilire se necessaria

Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;

Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;

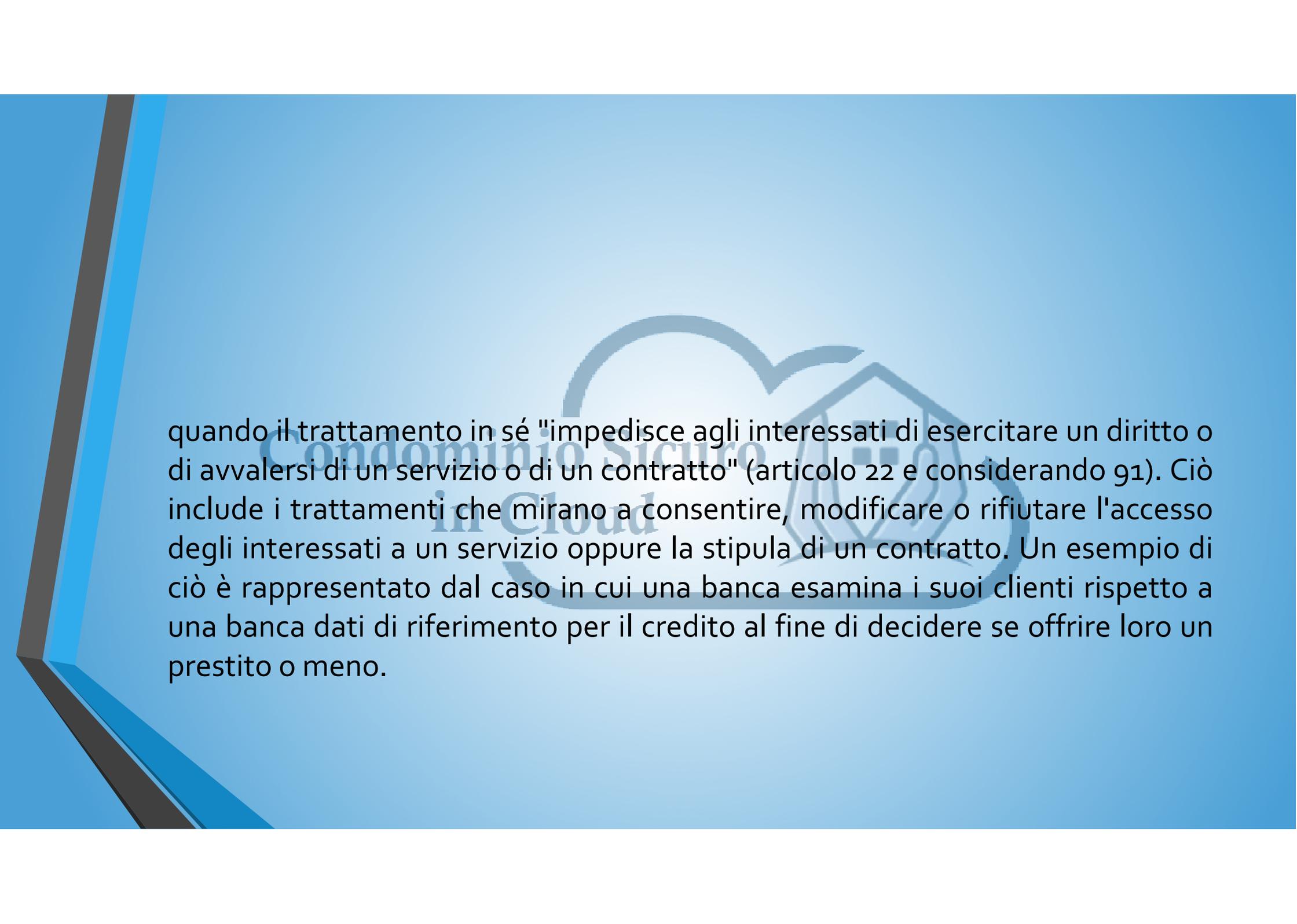
monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c)¹⁵. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche.

trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala¹⁶: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento;

dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;



quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Registro Dei trattamenti

Tutti i titolari e i responsabili di trattamento, **eccettuati gli organismi con meno di 250 dipendenti** ma solo se non effettuano trattamenti a rischio (*si veda art. 30, paragrafo 5*), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva** ("tra le altre, se del caso"). Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** (*ex art. 33 Codice*) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Notifica delle violazioni di dati personali

A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.

TRASFERIMENTO DATI VERSO ALTRI PAESI

Il regolamento *(si veda Capo V)* ha confermato l'approccio attualmente vigente per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

- i) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
- ii) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello);
- iii) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

T-Box

- Cloud residente su server locale, garantisce la permanenza dei dati su server europeo a differenza di quanto non viene garantito dalle maggiori piattaforme cloud (es. dropbox, onedrive, gdrive, iCloud)



Attenzione ai server utilizzati dai sistemi di videosorveglianza!

Condominio Sicuro
in Cloud

- E a compilare in modo corretto i cartelli.....

