click
software gestione condominio

FREE WEBINAR

Mercoledì 16 maggio 2018 – ore 12:00

25.05.2018

GDPR

General Data Protection Regulation

Regolamento UE 2016/679

Cosa significa e cosa cambia dal 25 maggio 2018

AGENDA

- ❑ Introduzione al nuovo Regolamento UE 2016/679
- ❑ Gli aspetti legali del GDPR
- ❑ L' Analisi dei Rischi
- ❑ Come prepararsi al GDPR

click
software gestione condominio

Introduzione al nuovo Regolamento UE 2016/679

Le principali novità del GDPR

Dott. Biagio LEVRINI

Perché un Regolamento Europeo ?

Perché il Mondo è cambiato

Evoluzione della Tecnologia

Sviluppo dell'Economia Digitale

Difficoltà a garantire efficacemente la protezione dei dati personali dei cittadini

Necessità di regole uniformi in tutti i Paesi EU

Diritto alla Privacy
(limite alla libertà di informazione)

Diritto alla protezione dei dati personali
(difesa dal controllo sulle persone)

DATI PERSONALI → LIBERTÀ E DIRITTI

click
software gestione condominio

Il GDPR in breve

- **General Data Protection Regulation** (GDPR) è il Regolamento Europeo 2016/679 che riguarda la **Protezione dei dati personali delle Persone fisiche**
- **Aggiorna e abroga la "Direttiva Madre" (95/46/CE),** ormai superata (recepita dall'attuale D.Lgs 196/2003, il c.d. Codice Privacy)
- È stato realizzato per **potenziare e unire i diritti sulla Privacy online e la Protezione dei dati personali all'interno dell'Unione Europea** (EU) e al tempo stesso velocizzare gli obblighi delle imprese al servizio dei cittadini EU
- **Amplia il concetto di dato personale** - qualunque tipo di informazione riferita/riferibile a persona **indipendentemente dal contesto** (privato/vita familiare o altra attività); **dalla forma** (caratteristiche, es. alfabetica, numerica, fotografica, acustica); **dal supporto** (carta, HD, video, ecc.)
- **Si applicherà in maniera ubiquitaria in tutti i 27 paesi EU**, mediante **un unico Regolamento al posto delle attuali leggi nazionali** a partire **dal 25 Maggio 2018** (NOTA: il GDPR è già in vigore dal 24 Maggio 2016).

click
software gestione condominio

E’ una nuova Legge Privacy ?

No, è molto di più, poiché l’approccio è differente:

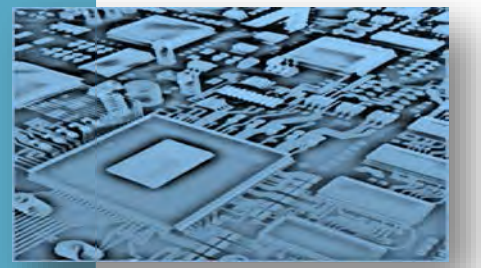
- Il **D.lgs. 196/2003**, la cosiddetta “Legge Privacy”, aveva abituato le aziende italiane ad una serie di **prescrizioni puntuali**, le famose checklist, a cui ottemperare.
- Il **GDPR**, invece, non indica le linee guida per proteggere le informazioni, ma **chiede alle aziende di dimostrare di averle protette in modo adeguato**.
- Pertanto **l’analisi del rischio privacy** assume un ruolo fondamentale: diventa lo strumento per dimostrare che le **misure implementate sono adeguate all’obiettivo principe di tutela dei dati trattati**.

click
software gestione condominio

Obiettivi del GDPR

- **ADEGUARE** le norme al contesto tecnologico attuale
- **RINFORZARE i Diritti delle persone** garantendo che i dati siano raccolti e gestiti sono nei casi e negli ambiti davvero necessari
- **GARANTIRE che di dati** personali dei cittadini europei **siano sempre protetti** con adeguati sistemi di sicurezza
- **REGOLAMENTARE** le loro modalità di **trattamento, conservazione e distruzione** quando non sono più richiesti
- **UNIFORMARE** la normativa in tutta l'Unione Europea
- **STABILIRE sanzioni importanti** in caso di violazione del Regolamento

click
software gestione condominio



DSC Digital System Computers
Soluzioni ICT dal 1981

Il tuo Amico Informatico

- Sistemi SaaS/IaaS

System Integration

WEB

BI

FLEET MANAGEMENT

Sistemi ERP tailor-made

SOLUZIONI SU MISURA

Backup e DR

HOUSING

RFid

Assistenza sistemistica

Consulenza IT

click
software gestione condominio

Cosa stiamo facendo

Essere GDPR «compliant»

Dopo aver analizzato le nuove regole abbiamo creato **un team di esperti del GDPR** composto da esperti informatici, legali, consulenti nella gestione del rischio

click
software gestione condominio

dsc
digital system computers

Gli aspetti legali del GDPR

Novità, adempimenti, obblighi e sanzioni

Avv. Giacomo ALLI

click
software gestione condominio

Sintetizzando…

- Il GDPR non è la 'nuova legge sulla privacy', ossia non abroga in toto il vecchio D.lgs 196/2003 ma ne rivede le finalità estendendo, tra le altre cose, il concetto di '**protezione dei dati personali**'.
- Il GDPR è una legge che **riguarda tutte le aziende che lavorano in Europa**, ovunque siano site, sia pubbliche che private, indipendentemente dalla dimensione.
- Il GDPR **non potrà subire** '**deroghe**' poiché non dovrà essere recepito dalla nostra legislazione nazionale
- Il GDPR **si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali**

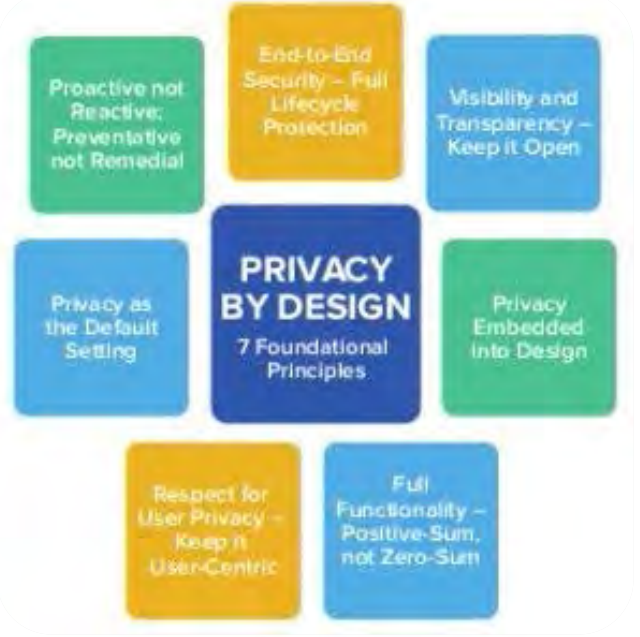
click
software gestione condominio

I principi fondamentali del GDPR

Accountability

Trasparenza

Privacy by design



Alcuni concetti importanti (Art.4 del regolamento UE 2016/679)

- **Dato personale**: «qualsiasi i**nformazione 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».
- **Dato particolare** (Dato sensibile per il *Codice Privacy*): **informazioni particolari relative alle persone** e ad informazioni genetiche➔ biometriche➔ relative alla salute➔ a condanne penali ed ai reati o a connesse misure di sicurezza (non esiste una lista ma solo dei criteri).
- **Profilazione**: «**qualsiasi forma di trattamento automatizzato di dati personali** consistente **nell'utilizzo di tali dati personali per valutare** determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»;

Principi da rispettare

- **Principio di liceità, correttezza e trasparenza**;
- **Principio di limitazione delle finalità**: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modi non incompatibili con tali finalità iniziali (ad esclusione delle raccolte per interesse pubblico, scientifico, statistico o storico);
- **Principio di minimizzazione dei dati**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Principio dell'esattezza**: i dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati
- **Principio della limitazione della conservazione**: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (fanno eccezione, come prima menzionato, quelli raccolti per interesse pubblico);
- **Principio dell'integrità e della riservatezza**: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- **Principio della responsabilizzazione**: Il titolare del trattamento è competente per il rispetto dei principi ora evidenziati e deve essere in grado di comprovarlo.

click
software gestione condominio

I soggetti che trattano Dati

1) **INTERESSATO** (Data Subject): persona fisica a cui si riferiscono i dati
2) **TITOLARE DEL TRATTAMENTO** (Data Controller): decide mezzi e finalità del trattamento (solitamente è il legale rappresentante dell'azienda)
3) **RESPONSABILE DEL TRATTAMENTO** (Data Processor): tratta dati per conto del Data Controller (es. titolare dell'azienda fornitore del sistema gestionale in cloud)
4) **INCARICATO DEL TRATTAMENTO** (Authorised): persona fisica dipendente dalle figure n. 2 o 3 (Titolare/Responsabile)
5) **DESTINATARIO** (Recipient): chi riceve comunicazione di dati (es. titolare dell'azienda produttrice del software gestionale con cui si gestiranno i dati)
6) **DATA PROTECTION OFFICER (DPO):** non obbligatorio sotto i 250 dipendenti, si occupa di considerare i rischi inerenti al trattamento, «coadiuvare» il Titolare

click
software gestione condominio

Diritti degli interessati:

ACCESSO: Avere conferma che sia in corso un trattamento di dati e accesso agli stessi (copia)
RETTIFICA: Ottenere la correzione o integrazione dei dati personali inesatti
LIMITAZIONE DEL TRATTAMENTO: Richiedere la sola conservazione (illiceità del trattamento, mancata correttezza dei dati, particolare necessità dell'interessato)
PORTABILITÀ: Ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico e richiederne trasmissione ad altro titolare del trattamento
OBLIO: Decidere che siano cancellati tutti i dati personali non più necessari alle finalità
OPPOSIZIONE: Opporsi in qualsiasi momento al trattamento automatizzato che abbia impatti significativi sulla sua libertà o diritti, compresa la profilazione
RECLAMO: Reclamare all'Autorità Garante la Privacy per ogni presunta violazione del GDPR
RICORSO GIURISDIZIONALE: Ricorrere in giudizio contro il Titolare ed eventuali responsabili del trattamento per violazioni al trattamento dei propri dati

click
software gestione condominio

Trasparenza del trattamento: **L'informativa**

- Deve essere **concisa, trasparente, intellegibile, semplice e chiara**.
- **Deve essere sempre resa** (anche non per iscritto) e **con mezzi comprovanti l'identità** dell'interessato.


FAC-SIMILE modello di INFORMATIVA

Click s.r.l.
Sede legale e operativa: Via XX Settembre 30 20025 Legnano
P.IVA / C.F. 08144530964
www.clicksrl.eu info@clicksrl.eu

8) TRASFERIMENTO DEI DATI

I dati personali sono conservati su server ubicati [...], all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server anche extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali standard previste dalla Commissione Europea.

7) NATURA DEL CONFERIMENTO DATI E CONSEGUENZE DEL RIFIUTO DI RISPONDERE

Il conferimento dei dati per le finalità di cui all'art. 2.A) è obbligatorio. In loro assenza, non potremo garantirLe i Servizi dell'art. 2.A). Il conferimento dei dati per le finalità di cui all'art. 2.B) è invece facoltativo. Può quindi decidere di non conferire alcun dato o di negare successivamente la possibilità di trattare dati già forniti: in tal caso, non potrà ricevere newsletter, comunicazioni commerciali e materiale pubblicitario inerenti ai Servizi offerti dal Titolare. Continuerà comunque ad avere diritto ai Servizi di cui all'art. 2.A).

6) DIRITTI DELL'INTERESSATO

Nella Sua qualità di interessato, ha i diritti di cui all'art.7 Codice Privacy e art. 15 GDPR e precisamente i diritti di:
i. Ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
ii. Ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2 Codice Privacy e art. 3, comma 1, GDPR; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
iii. Ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
iv. Opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che La riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, mediante l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore mediante e-mail e/o mediante modalità di marketing tradizionali mediante telefono e/o posta cartacea. Si fa presente che il diritto di opposizione dell'interessato, esposto al precedente punto b), per finalità di marketing diretto mediante modalità automatizzate si estende a quelle tradizionali e che comunque resta salva la possibilità per l'interessato di esercitare il diritto di opposizione anche solo in parte. Pertanto, l'interessato può decidere di ricevere solo comunicazioni mediante modalità tradizionali ovvero solo comunicazioni automatizzate oppure nessuna delle due tipologie di comunicazione. Ove applicabili, ha altresì i diritti di cui agli artt. 16-21 GDPR (Diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione), nonché il diritto di reclamo all'Autorità Garante.

9) MODALITÀ DI ESERCIZIO DEI DIRITTI

Potrà in qualsiasi momento esercitare i diritti inviando:
- una raccomandata a.r. a [...] – Sede operativa presso [...] – indirizzo – cap, luogo;
- una e-mail all'indirizzo [...].

10) TITOLARE, RESPONSABILE ED INCARICATI

Il Titolare del trattamento è **D.S.C. digital system computers Srl**, con sede legale in Via XX Settembre 30, 20025 LEGNANO (MI) e sede operativa presso [...] (inserire se indirizzo diverso da sede legale).

L'elenco aggiornato dei responsabili e degli incaricati al trattamento è custodito presso la sede legale del Titolare del trattamento.

click
software gestione condominio

L'informativa
Il nuovo modello

Deve contenere almeno:

- ✓**Identità e contatti del titolare** (e del responsabile se presente)
- ✓**Finalità del trattamento**, eventuali destinatari, eventuali trasferimenti
- ✓**Periodo di conservazione**
- ✓**Diritti dell'interessato** (tra cui revoca del consenso e diritto di reclamo)
- ✓Eventuale esistenza di un **processo decisionale automatizzato**
- ✓Se non raccolti presso l'interessato, anche la **categoria di dati e la fonte**


FAC-SIMILE modello di INFORMATIVA

Click s.r.l.
Sede legale e operativa: Via XX Settembre 30 20025 Legnano
P.IVA / C.F. 08144530964
www.clicksrl.eu info@clicksrl.eu

6) TRASFERIMENTO DEI DATI

I dati personali sono conservati su server ubicati [...], all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server anche extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili, previa stipula delle clausole contrattuali standard previste dalla Commissione Europea.

7) NATURA DEL CONFERIMENTO DATI E CONSEGUENZE DEL RIFIUTO DI RISPONDERE

Il conferimento dei dati per le finalità di cui all'art. 2.A) è obbligatorio. In loro assenza, non potremo garantirLe i Servizi dell'art. 2.A). Il conferimento dei dati per le finalità di cui all'art. 2.B) è invece facoltativo. Può quindi decidere di non conferire alcun dato o di negare successivamente la possibilità di trattare dati già forniti: in tal caso, non potrà ricevere newsletter, comunicazioni commerciali e materiale pubblicitario inerenti ai Servizi offerti dal Titolare. Continuerà comunque ad avere diritto ai Servizi di cui all'art. 2.A).

8) DIRITTI DELL'INTERESSATO

Nella Sua qualità di interessato, ha i diritti di cui all'art.7 Codice Privacy e art. 15 GDPR e precisamente i diritti di:
i. Ottenere la conferma dell'esistenza o meno di dati personali che La riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
ii. Ottenere l'indicazione: a) dell'origine dei dati personali; b) della finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2 Codice Privacy e art. 3, comma 1, GDPR; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
iii. Ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
iv. Opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che La riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, mediante l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore mediante e-mail e/o mediante modalità di marketing tradizionali mediante telefono e/o posta cartacea. Si fa presente che il diritto di opposizione dell'interessato, esposto al precedente punto b), per finalità di marketing diretto mediante modalità automatizzate si estende a quelle tradizionali e che comunque resta salva la possibilità per l'interessato di esercitare il diritto di opposizione anche solo in parte. Pertanto, l'interessato può decidere di ricevere solo comunicazioni mediante modalità tradizionali ovvero solo comunicazioni automatizzate oppure nessuna delle due tipologie di comunicazione. Ove applicabili, ha altresì i diritti di cui agli artt. 16-21 GDPR (Diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione), nonché il diritto di reclamo all'Autorità Garante.

9) MODALITÀ DI ESERCIZIO DEI DIRITTI

Potrà in qualsiasi momento esercitare i diritti inviando:
- una raccomandata a.r. a [...] – Sede operativa presso [...] – indirizzo – cap, luogo;
- una e-mail all'indirizzo [...].

10) TITOLARE, RESPONSABILE ED INCARICATI

Il Titolare del trattamento è **D.S.C. digital system computers Srl**, con sede legale in Via XX Settembre 30, 20025 LEGNANO (MI) e sede operativa presso [...] (inserire se indirizzo diverso da sede legale).

L'elenco aggiornato dei responsabili e degli incaricati al trattamento è custodito presso la sede legale del Titolare del trattamento.

FAC-SIMILE modello d

INFORMATIVA PER IL TRATTAME

Click Srl, con sede legale in Via XX Settembre 30, 20025 LEGNANO (
di titolare del trattamento, La informa ai sensi dell'art. 13 D.Lgs. 30.6
Regolamento UE n. 2016/679 (di seguito, "**GDPR**") che i Suoi dati sa

1) OGGETTO DEL TR

Il Titolare tratta i dati personali, identificativi (ad esempio, nome, cogn
bancari e di pagamento - in seguito, "dati personali" o anche "dati") da
per i servizi del Titolare.

2) FINALITA' DEL TR

I Suoi dati personali sono trattati:
A) senza il Suo consenso espresso (art. 24 lett. a), b), c) Codice Pri
Servizio:
- Concludere i contratti per i servizi del Titolare;
- Adempiere agli obblighi precontrattuali, contrattuali e fiscali derivant
- Adempiere agli obblighi previsti dalla legge, da un regolamento, dall
ad esempio in materia di anticiclaggio);
- Esercitare i diritti del Titolare, ad esempio il diritto di difesa in giudi
B) Solo previo Suo specifico e distinto consenso (artt. 23 e 130 C
Marketing;
- inviarLe via e-mail, posta e/o sms e/o contatti telefonici, newsletter,
prodotti o servizi offerti dal Titolare e rilevazione del grado di soddisfa
- inviarLe via e-mail, posta e/o sms e/o contatti telefonici comunicazi
Le segnaliamo che se siete già nostri clienti, potremo inviarLe comuni
analoghi a quelli di cui ha già usufruito, salvo Suo dissenso (art. 130

3) MODALITA' DI TR

Il trattamento dei Suoi dati personali è realizzato per mezzo delle op
GDPR e precisamente: raccolta, registrazione, organizzazione, cor
selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, co
dati personali sono sottoposti a trattamento sia cartaceo che elettroni
Il Titolare tratterà i dati personali per il tempo necessario per adempi
anni dalla cessazione del rapporto per le Finalità di Servizio e per r
Marketing.

4) ACCESSO AI DATI

I Suoi dati potranno essere resi accessibili per le finalità di cui all'art. 2.A) e 2.B):
- a dipendenti e collaboratori del Titolare, nella loro qualità di incaricati e/o responsabili interni del trattamento e/o amministratori di sistema;
- a società terze o altri soggetti (a titolo indicativo, istituti di credito, studi professionali, consulenti, società di assicurazione per la prestazione di servizi assicurativi, etc.) che svolgono attività in outsourcing per conto del Titolare, nella loro qualità di responsabili esterni del trattamento.

5) COMUNICAZIONE DEI DATI

Senza la necessità di un espresso consenso (ex art. 24 lett. a), b), d) Codice Privacy e art. 6 lett. b) e c) GDPR), il Titolare potrà comunicare i Suoi dati per le finalità di cui all'art. 2.A) a Organismi di vigilanza, Autorità giudiziarie, a società di assicurazione per la prestazione di servizi assicurativi, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle finalità dette. Detti soggetti tratteranno i dati nella loro qualità di autonomi titolari del trattamento. I Suoi dati non saranno diffusi.

Trasparenza del trattamento: **Il consenso**

Non è necessario solo se i dati sono conferiti:

- **per l'esecuzione di un contratto**
- **per obblighi legali del titolare**
- **per la salvaguardia degli interessi vitali di un terzo**
- **per interesse pubblico**
- **per interesse legittimo del titolare**

Deve essere richiesto in linguaggio semplice e chiaro, specificamente (per finalità) ed essere chiaramente distinguibile, comprensibile, facilmente accessibile.

Non deve essere necessariamente scritto ma **deve essere dimostrabile**

Per **categorie particolari di dati** e per le **decisioni con trattamento automatizzato** deve essere **esplicito**.

Gli obblighi di Legge
Il Data Breach

Qualsiasi violazione dei dati personali deve essere documentata, quando il titolare ne viene a conoscenza (registro degli incidenti).

Se la violazione presenta rischi per i diritti e le libertà delle persone, il titolare è tenuto a notificarla alla Autorità di controllo entro 72 ore (il responsabile informa il titolare senza ritardo).

Se la violazione presenta alti rischi per i diritti e le libertà delle persone, il Titolare è tenuto ad informare anche gli interessati in modo chiaro, semplice e immediato e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Per essere documentata e poi notificata la violazione deve essere intercettata, dunque **deve essere progettata e implementata una serie di misure di prevenzione, monitoraggio, controllo su violazioni**.

La notifica deve descrivere la natura della violazione - Comunicare i riferimenti di un punto di contatto - Descrivere le probabili conseguenze della violazione - Descrivere le misure adottate o proposte per porre rimedio alla violazione e attenuarne i possibili effetti negativi

Gli obblighi di Legge
Il Data Breach

Il Titolare del trattamento **potrà decidere di non informare gli interessati**:

- se riterrà che la violazione non comporti un rischio elevato per i loro diritti
- dimostrerà di avere adottato misure di sicurezza a tutela dei dati violati (e.g. cifratura)
- sosterrà che informare gli interessati comporta uno sforzo sproporzionato, nel qual caso è richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile

L'Autorità di controllo potrà comunque imporre al Titolare del trattamento di informare gli interessati sulla base di una autonoma valutazione del rischio associato alla violazione.

Il GDPR
Le sanzioni

- **Sanzioni Amministrative pecuniarie**: due fasce
- **Fascia bassa** (Violazione di OBBLIGHI): fino a €10Mio o 2% fatturato annuo globale se superiore (obblighi relativi alle figure responsabili del trattamento dei dati / obblighi relativi al trattamento di dati di minori)
- **Fascia alta** (violazione di DIRITTI): fino a €20Mio o 4% fatturato annuo globale se superiore (Violazione di principi di base del trattamento/condizioni relative al consenso/diritti degli interessati/trasferimenti)

- **Cumulo giuridico in caso di più violazioni** (art. 83.3)
- **Criteri per graduare la sanzione**
- **Non sono previste soglie minime**

- **Sanzioni Penali** (legge di ogni singolo Stato Membro)

Come prepararsi al GDPR
L'esperienza di DSC e Click

Dott. Biagio LEVRINI

Il GDPR
Come prepararsi (in sintesi)

- **Identificare** quali dati sono utilizzati e come sono protetti e conservati in azienda (back-up)
- **Creare** un sistema di responsabilità chiare
- **Adottare** il GDPR come parte integrante delle procedure di tutta l'azienda per avvalersi dell'occasione come opportunità di miglioramento
- **Aggiornare** e **verificare periodicamente** policies e procedure
- **Prepararsi** anche alle situazioni di rischio (Data Breach)

click
software gestione condominio

Il GDPR
Un rischio da valutare

- Ogni imprenditore conosce la propria azienda più di ogni altro e **definisce il livello di rischio accettabile** per il business aziendale
- **Promuove le azioni adeguate a fronteggiare e ridurre i rischi**, legati alla sicurezza delle informazioni, e i possibili danni dovuti ad eventuali violazioni

Ma dove sono i dati ?
Chi li usa?
Come ?

Normalmente **ogni azienda/organizzazione decide quanto è disposta a «rischiare»** rispetto all'impatto del realizzarsi di una minaccia.

C’era una volta…

Con i faldoni era molto più semplice …
bastava un armadio con serratura!

Ma oggi:

- Cloud Computing
- Social Network,
- Smartphone, tablet,
- IoT, Big Data, Sentiment Analysis…

Come proteggersi ?

click
software gestione condominio

Cosa dobbiamo considerare
Gli adempimenti del GDPR

- I principali adempimenti previsti dal GDPR:
  - **Aggiornamento delle informative e raccolta dei consensi** per il trattamento dei dati personali
  - **Regolamentazione dei rapporti** tramite nomina e/o contratto con i Responsabili del trattamento che operano per conto del Titolare
  - Se previsto, nomina di un **Data Protection Officer** (DPO)
  - **Valutazione d'impatto** quando un trattamento comporta rischi per i diritti e le libertà degli interessati - Data Protection Impact Assessment (DPIA)
  - **Adozione di misure di sicurezza adeguate** al trattamento, alle finalità, ai costi di attuazione e ai rischi individuati
  - **Predisposizione del Registro dei Trattamenti**, se previsto e/o ritenuto utile
  - Rispetto dei principi di «protezione dei dati personali già dalla fase di progettazione» (***privacy by design***) e «raccolta e trattamento, per impostazione predefinita, solo dei dati necessari alle finalità» (***privacy by default***)
  - **Obbligo di notifica** all'Autorità Garante e ai soggetti interessati, nei casi peggiori, qualora si verifichi una violazione dei dati personali (***data breach***)

Cosa dobbiamo considerare

Le informazioni hanno valore non solo per gli interessati ma anche per l'azienda che li tratta

Tutti i soggetti coinvolti nell'azienda traggono **Valore dalle informazioni** per:

- **Fare scelte migliori**
- **Lavorare in modo più produttivo ed efficiente.**

L'informazione in un'azienda ha **valore in ragione della sua utilità** per i suoi diversi scopi.

Un errore comune è **percepire il valore delle informazioni solo nel momento in cui non sono più disponibili** (es. furto notebook deve far pensare ai dati che vi erano contenuti e non al valore dell'oggetto)

Quindi i dati vanno protetti in modo adeguato **per avere la garanzia sulla loro:**

- **Integrità**
- **Disponibilità**
- **Riservatezza**

click
software gestione condominio

I danni derivanti da furto/perdita di dati
Danni spesso difficili da valutare

Costi per:

- **Implicazioni giuridiche** (Cause legali dopo furto/perdita di dati personali)
- **Sanzioni per violazione delle nuove regole**
- **Perdite finanziarie** (es. furto di denaro mediante clonazione carte di credito – 2° causa di perdita causata dal crimine informatico)
- **Furto di Informazioni di business** (3° fonte di guadagno per il crimine informatico)
- **Perdita di business** (realizzazione immediata di un affare e rischio di allontanamento dei clienti – es. sito e-commerce)
- **Costi per la perdita di produttività**
- **Danno alla Brand Reputation**

La formazione del personale prima di tutto…

Qualche suggerimento base…stare in guardia!

- **Non farsi indurre con l'inganno a rivelare informazioni riservate** (solitamente via telefono e/o mail)
- **Evitare di usare un pc non protetto** (password di accesso, antivirus, personal firewall, …)
- **Evitare di lasciare in giro informazioni personali** (fogli sulla scrivania, pendrive, hard disk)
- **Bloccare PC, smartphone, tablet quando non sono in uso e non condividere le proprie credenziali di accesso con altri** (colleghi di lavoro ed altri)
- Fogli di riciclo (?)
- **Proteggere con password dispositivi e file di natura sensibile**
- **Usare password complesse** (password, 1234, nome → non sono sicure)
- **Prestare attenzione agli allegati** nelle e-mail e ai link sospetti
- **Evitare di installare programmi non autorizzati** sui PC del lavoro
- **Effettuare il backup dei dati** con una periodicità definita in relazione alla loro variazione

click
software gestione condominio

Un suggerimento per tutti

Non considerare l'Analisi dei Rischi Privacy **un'attività di competenza esclusiva dei Sistemi Informativi / Reparti IT**.

L'analisi infatti, deve **tener conto di tutti i processi ed asset** coinvolti nel trattamento, **anche quelli non informatici**.

Occorre proteggere i data center, i server ed i database in essi contenuti, tanto quanto i faldoni ed i locali in cui essi sono conservati !

click
software gestione condominio

E poi considerare la situazione specifica…

Misure adeguate a dati e contesto aziendale

Le misure a tutela del trattamento da attuare **dipendono**

- **sia dalla natura** del trattamento stesso
- **sia dalle caratteristiche del Titolare del trattamento dati**

Una grande azienda (o magari una multinazionale) probabilmente avrà una capacità di spesa che le consentirà di accedere a soluzioni di mercato «top» diverse da quelle di una MPMI.
Per questa ragione misure adottate da una MPMI a tutela dei trattamenti e ritenute idonee, potrebbero invece essere giudicate insufficienti per una grossa azienda.

Cosa incominciare a fare
Identificare quali dati, chi li usa, come li protegge

Il GDPR prevede la creazione del **Registro dei trattamenti** (art. 30): in questo documento ci deve essere almeno l'elenco dei trattamenti svolti dal Titolare, i processi a cui afferiscono e gli asset coinvolti nel trattamento oltre a quanto prescritto dal comma 1 dell'art. 30, rispetto alla natura dei dati trattati.

A partire da queste informazioni è possibile integrare le **analisi del rischio** esistenti o crearne una ad-hoc per la Data Protection, **tenendo sempre ben presente che l'ottica deve essere quella dell'interessato**.

Nel caso di Micro e Piccole Imprese è opportuno procedere per gradi, iniziando con la creazione di un **registro** che contenga i riferimenti a tutti i dati personali trattati, il motivo del trattamento e la loro gestione **(registro dei trattamenti)**.

click
software gestione condominio

Cosa incominciare a fare: l'Analisi dei Rischi

Il Registro dei trattamenti

Processi
- A quali processi aziendali sono necessarie queste informazioni

Tipologia dei dati
- Quali informazioni gestisco, a quale fine

Asset
- Quali strumenti vengono usati per l'esecuzione dei processi

Analisi del rischio
- Quali rischi sul trattamento, come li rendo accettabili

Quali dati raccogliamo ?
Come li raccogliamo?
Per quali finalità?
Come li trattiamo e per quanto tempo?
Chi sono i soggetti interni ed esterni coinvolti?
Come li proteggiamo e conserviamo?

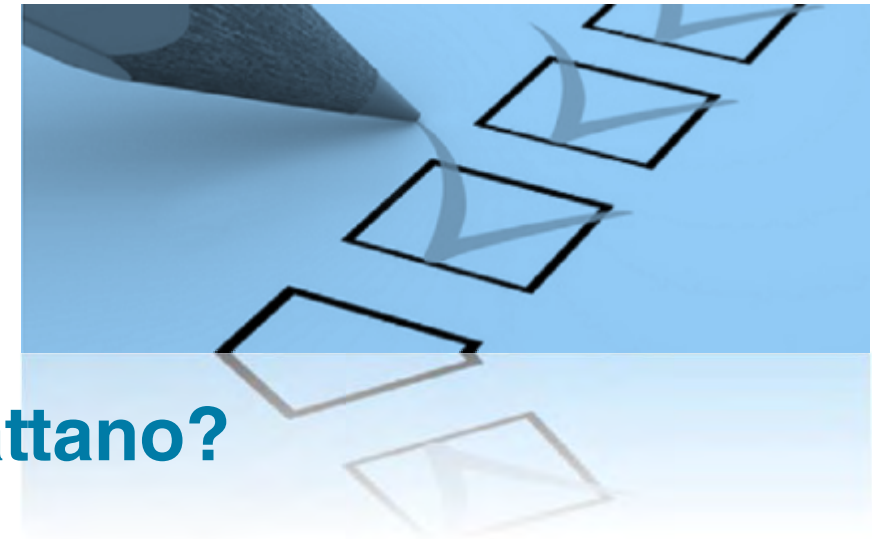
click
software gestione condominio

Cosa sta facendo CLICK

Vivere il GDPR come un'opportunità di miglioramento

- **Formalizzazione processi/definizione responsabilità/analisi dei rischi**
- Verifica dei punti deboli
- Analisi delle lacune
- **Determinazione delle priorità di intervento** (Datacenter, Software)
- **Revisione contratti/accordi** (informativa, accordi riservatezza/NDA, contratti)
- **Creazione di una nuova policy per BYOD e collaboratori esterni**
- **Formazione del personale interno** (promozione di una cultura del dato)
- **Comunicazione anche verso i clienti**

Che dati abbiamo ?
Perché ci servono?
Come li proteggiamo?
Come li conserviamo?
Chi sono i soggetti che li trattano?



GDPR e Condominio
I punti chiave in sintesi

- **L'amministratore può trattare i dati dei condomini**
- **I dati trattati devono essere quelli indispensabili** all'adempimento del contratto (ogni dato ulteriore previo consenso)
- **L'amministratore deve fornire idonea informativa** aggiornata al GDPR (condomini/terzi)
- **Lo studio dell'amministratore deve essere adeguato ed organizzato in termini di sicurezza fisica e tecnologica** (documenti non accessibili al pubblico, firewall, antivirus, ecc.)

click
software gestione condominio

Il Datacenter DSC: un datacenter a km 0

Come proteggiamo i dati dei nostri clienti

Il Datacenter DSC:

- ❑ **Sicuro**: segregazione REI 120
  sistema di controllo accessi Ksenia Security
  Servizio sorveglianza da Mondialpol Vedetta 2
- ❑ **Controllato**: sistemi di Alimentazione, Raffreddamento e Monitoraggio ridondati – Collegato alla fibra ottica
- ❑ **In House**: completamente gestito da tecnici DSC (capacità di intervento h 24 - 7/7)

SAAS
IAAS
PAAS
HOSTING
HOUSING
BACK-UP & DR

click
software gestione condominio

Cosa sta facendo DSC

Gli interventi su sw e nuovi servizi

- **Policy di gestione delle credenziali di accesso**
- **Analisi e verifica delle modalità di connessione** rispetto ai dati trattati
- **Verifica per l'introduzione di soluzioni di crittografia** (dati incomprensibili) **ed pseudonimizzazione** (dati anonimi)
- **Servizi di Back-up remoto e sicurezza ICT**
- **Formazione del personale interno**
- **Formazione verso i clienti**

Condominoclick.it

Linked

Il CLICK/DSC GDPR team

Una squadra che può aiutare…

- ❑ **Analisi dei rischi**
- ❑ **Progettazione del sistema GDPR**
- ❑ **Implementazione delle soluzioni ICT a protezione dei dati**
- ❑ **Supporto per il costante aggiornamento organizzativo/ tecnologico**
- ❑ **Monitoraggio ed audit**

…ad essere GDPR compliant

dsc digital system computers

click software gestione condominio

Il DSC GDPR team

La proposta di supporto per la GDPR compliance

- **GDPR Compliance**

Risk assessment/DPIA/Definizione procedure e controlli/formazione personale
intervento ca. 35 ore
(tariffa riservata ai clienti CLICK/DSC Euro 35/ora)

click
software gestione condominio

Riferimenti per approfondimento

Per approfondire ulteriormente

1997 2017

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

www.garanteprivacy.it

click
software gestione condominio

Tante grazie per l’attenzione

Ing. Simone CORDANO - simone.cordano@clicksrl.eu – CEO