Collegio Geometri e Geometri Laureati
della Provincia di Reggio Emilia

LA GESTIONE DELLA PRIVACY AI SENSI DEL REGOLAMENTO EUROPEO 2016/679:

Novità e adempimenti per i professionisti ed imprese

Reggio Emilia, 7 giugno 2018

LA PRIVACY NELLO STUDIO TECNICO E NEI RAPPORTI DI LAVORO

Dott.ssa LUCIANA BRUNO

Consulente del lavoro

Entrata in vigore ed efficacia del Regolamento

COSA STA' ACCADENDO DAL 25 MAGGIO 2018 ?

Definizione di DATO PERSONALE

Art. 4 parag. 1

qualsiasi **informazione riguardante**
una persona fisica identificata o identificabile (“*interessato*”):

Valore del dato personale

- La gestione di dati personali può essere utile o necessaria per scopi amministrativi o commerciali
- Inoltre, i dati personali hanno un valore di mercato.
- Tuttavia, le violazioni nella riservatezza dei dati personali possono causare danni fisici, materiali e morali
- Quindi, vi è interesse ad acquisirli legalmente o meno perché possono essere sfruttati per:
  - ✓ marketing (es., spam, pubblicità commerciale e politica)
  - ✓ violazioni diritti e libertà civili(es., discriminazione, rifiuto di accesso alle prestazioni, licenziamento)
  - ✓ azioni criminali (es., truffe, furto di identità, diffamazione, minacce, ricatti, furti, aggressioni)

I dati trattati
dal Collegio dei Geometri e Geometri Laureati

- cognome e nome,
- luogo e data di nascita,
- titolo di studio,
- residenza e domicilio professionale,
- data di iscrizione all'Ordine,
- gli estremi del diploma di abilitazione,
- indirizzo pec e indirizzo posta elettronica ordinaria,
- recapiti telefonici;
- annotazione eventuali provvedimenti disciplinari

Finalità dei dati trattati dal Collegio dei Geometri e Geometri Laureati

Il trattamento dei dati personali avviene per lo svolgimento delle funzioni istituzionali del Consiglio Direttivo sulla base di quanto disposto dalla Legge che regolamenta l'ordinamento professionale dei geometri

Il trattamento dei dati personali ha le seguenti finalità:
- tenuta ed aggiornamento dell'Albo professionale.

I dati trattati dal Geometra – professionista

EDILIZIA, URBANISTICA E AMBIENTE

Responsabile del servizio di prevenzione e protezione (RSPP), Addetto al servizio di prevenzione e protezione (ASPP)

Controllo del processo di sicurezza acustica

Progettazione lavori, Direzione lavori , Contabilità dei lavori, Collaudo dei lavori

Coordinamento della sicurezza in fase di progettazione dell'opera

Coordinamento della sicurezza in fase di esecuzione dell'opera

Redazione piano di recupero, Redazione piano di lottizzazione, Redazione piano del colore

Certificazione energetica

Consulenza per la qualificazione energetica degli edifici

Certificazione acustica degli edifici

Consulenza per la qualificazione acustica degli edifici

Progettazione e verifica ai fini della prevenzione incendi

Amministrazione immobiliare, Redazione piano di zonizzazione

trattamento dati «SENSIBILI»

categoria di dati ?

Dati «COMUNI»

I dati trattati dal Geometra – professionista

GEOMATICA E ATTIVITA' CATASTALE

Redazione tipo o piano di frazionamento
Redazione tipo mappale
Redazione tipo particellare
Denuncia al catasto fabbricati
Voltura catastale
Rilievo del territorio
Rilievo di fabbricati
Rilievo di precisione
Tracciamento di infrastrutture territoriali
Tracciamento di fabbricati
Tracciamento di lottizzazioni

I dati trattati dal Geometra – professionista

ESTIMO E ATTIVITA' PERITALE

Dati «GIUDIZIARI»

Valutazione immobiliare
Consulenza tecnica giudiziale, Consulenza tecnica stragiudiziale, Consulenza tecnica d'ufficio
Arbitrato
Redazione perizia contrattuale
Mediazione
Consulenza tecnica all'atto di trasferimento
Redazione tabelle millesimali
Riconfinazione
Redazione piano particellare di esproprio, Redazione della dichiarazione di successione
Redazione della dichiarazione di successione (Tavolare)
Accertamento usi civici
Due diligenze immobiliare
Audit documentale
Consulenza tecnica normativa

categoria di dati ?

Dati «COMUNI»

Il GDPR e D. Lgs. 196/03

- **Dove <u>non vi è compatibilità</u> tra quanto disposto dal Codice della Privacy e quanto previsto dal GDPR 679/2016, il Codice Privacy lascia il passo alle nuove disposizioni europee: la legge statale deve essere disapplicata in favore del GDPR**

- **Laddove vi sia <u>compatibilità tra le due norme</u>, il D. Lgs. 196/2003 rimane applicabile continuando a dettare legge, anche in maniera più specifica rispetto al GDPR (Enti Pubblici, accesso pubblico, lavoro, giornalismo …)**

Il Governo il 21/03/2018 ha presentato il testo del decreto legislativo alle Commissioni Parlamentari (Camera e Senato).

La delega scadeva il 21 maggio ma è stata prorogata, quindi **scadrà il 21 agosto 2018**

Schema del D. Lgs. recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679:

- ✓ **104 articoli**
- ✓ **Molti richiami a misure che deve adottare il Garante**
- ✓ **Autorità di controllo di cui all'art. 51 del GDPR è il Garante; ampia regolamentazione; si a linee guida, provvedimenti ed autorizzazioni generali; approvazione regole deontologiche**
- ✓ **Minore età = 14 anni per servizi della società dell'informazione;**
- ✓ **Persone decedute: diritti artt. 15-22 esercitati da eredi, testamento privacy?**
- ✓ **Tribunale ordinario: Rito del lavoro**
- ✓ **Curriculum = no consenso, si informativa successiva**
- ✓ **Parte speciale Settoriale** (scuola, lavoro, sanità, fini storici e statistici, comunicazioni elettroniche, telefonia ecc)
- ✓ **Art. 102: dall'entrata in vigore del decreto il dlgs196/2003 è abrogato + abrogati commi da 1021 a 1024 legge bilancio**

Rapporti tra GDPR 679/2016 e normativa Nazionale

- **Considerando n. 8 del GDPR**

Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale.

- **Considerando 10 del GDPR**

Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli «*Stati dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del presente regolamento*»

Rapporti tra GDPR 679/2016 e normativa Nazionale

- **Art. 6 paragrafo 2 del GDPR - liceità**

Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

- **Art. 9 paragrafo 4 del GDPR – dati sensibili**

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

GDPR 679/2016 - Efficacia territoriale

- **Il Titolare e Responsabile del trattamento stabiliti in uno Stato dell'Unione Europea indipendentemente dal fatto che il trattamento sia effettuato dall'Unione**

- **Il Titolare o Responsabile del trattamento non stabiliti nell'Unione Europea se trattano i dati personali di interessati che si trovano nell'Unione Europea, quando le attività di trattamento riguardano:**

a) l'offerta di beni o la prestazione di servizi agli interessati che si trovano nell'Unione

b) Il monitoraggio del loro comportamento che avvenga nell'Unione

GDPR 679/2016 - Efficacia soggettiva

OBBIGATI

- **Persone fisiche che trattano i dati per esigenze NON personali o familiari**
- **Persone giuridiche di diritto privato (con facilitazione per PMI)**
- **Enti pubblici e di diritto pubblico**

GDPR 679/2016 - Efficacia soggettiva

INTERESSATI

- **Persone fisiche**

DATI PARTICOLARI

Art. 9 parag. 1

1. **E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona**

2. **Casi in cui il divieto non si applica …**

PRINCIPI APPLICABILI AL TRATTAMENTO

Art. 5

DATI PERSONALI SONO:

A. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

B. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità;

C. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

D. 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 («esattezza»);

E. 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 … («limitazione della conservazione»);

F. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati/illeciti e dalla perdita, dalla distruzione o dal danno accidentale («integrità e riservatezza»).

LICEITA' DEL TRATTAMENTO DEI DATI

Art. 6

- consenso esplicito dell'interessato per finalità specifiche
- assolvimento obblighi in materia di diritto del lavoro e della sicurezza sociale
- per tutelare un interesse vitale dell'interessato
- dati trattati all'interno di una fondazione/associazione/organismo SENZA SCOPO DI LUCRO
- dati personali resi manifestatamente pubblici dall'interessato
- per accertare , esercitare o difendere un diritto in sede giudiziaria

… TRATTAMENTO DEI DATI

Art. 6

- per motivi di interesse pubblico
- per finalità di medicina preventiva, medicina del lavoro, valutazione delle capacità lavorative del dipendente
- per motivi di interesse pubblico nel settore della sanità pubblica ES. minacce gravi per la salute
- Per legittimo interesse del Titolare
- per fini statistici, storici e ricerca scientifica

LICEITA' DEL TRATTAMENTO – dati giudiziari

Art. 6

Trattamento relativo ai dati personali delle CONDANNE PENALI e dei reati o a connesse misure di sicurezza può avvenire solo sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati.

ALCUNE NOVITA' RILEVANTI

- **ACCOUNTABILITY**
- **PROTEZIONE SIN DALLA PROGETTAZIONE**
- **REGISTRO DEI TRATTAMENTI**
- **IL RESPONSABILE DELLA PROTEZIONE DEI DATI**

... ALCUNE NOVITA' RILEVANTI

- **RESPONSABILITA' SOLIDALE TRA TITOLARE E RESPONSABILE DEL TRATTAMENTO**
- **RESPONSABILITA' DEI CONTITOLARI**
- **DESIGNAZIONE DEL SUB-RESPONSABILE DEL TRATTAMENTO**
- **VIOLAZIONE DEI DATI (*DATA BREACH*)**

... ALCUNE NOVITA' RILEVANTI

- **<u>ELIMINAZIONE</u> DELL'OBBLIGO DI NOTIFICA AL GARANTE**
- **VALUTAZIONE D'IMPATTO**
- **CERTIFICAZIONI E CODICE ETICO**
- **DIRITTO ALL'OBLIO**

... ALCUNE NOVITA' RILEVANTI

- **TRATTAMENTO E CONSENSO PER I MINORI DI ANNI 16**
- **DIRITTO DI PORTABILITA' DEI DATI**
- **ENTITA' DELLE SANZIONI PARAMETRATE SUL FATTURATO**
- **PSEUDONIMIZZAZIONE : sostituzione del nome e cognome con codici**
- **PROFILAZIONE : qualsiasi forma di trattamento automatizzato**

I SOGGETTI DEL TRATTAMENTO

(dall'art. 24 all'art. 30 del Regolamento UE)

I SOGGETTI COINVOLTI NEL GDPR

DATA CONTROLLER **o**

TITOLARE DEL TRATTAMENTO

JOINT CONTROLLER **o**

CO-TITOLARI DEL TRATTAMENTO (Co-Responsabili)

DATA PROCESSOR **o**

PERSONE AUTORIZZATE AL TRATTAMENTO

DATA PROTECTION OFFICER (DPO) **o**

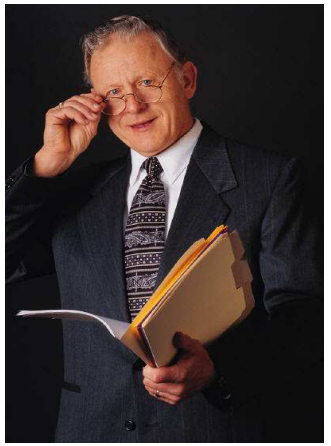
RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

Soggetto interessato (DATA SUBJECT)

IL TITOLARE "DATA CONTROLLER"

Art. 4 parag. 7

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



COMPETENZE

... IL TITOLARE

Adotta politiche e attua **le misure adeguate** per garantire ed essere in grado di dimostrare che il trattamento dati è conforme al Regolamento.

E' il soggetto tenuto all'accountability .

Ha il compito di attuare d'intesa col Responsabile del Trattamento la privacy by design e by default.

L'applicazione di codici di condotta o di un meccanismo di certificazione sono ELEMENTI per dimostrare il rispetto degli obblighi.

IL CONTITOLARE
"JOINT CONTROLLERS"

Art. 26

due o più titolari operano come contitolari del trattamento (determinando congiuntamente finalità e mezzi del medesimo), concordano in modo trasparente, mediante un contratto, la ripartizione delle responsabilità del trattamento, con particolare riguardo all'esercizio dei diritti degli interessati e ai connessi obblighi informativi. Il contenuto essenziale dell'accordo deve essere messo a disposizione degli interessati i quali possono rivolgersi all'uno o all'altro indifferentemente

RESPONSABILE DEL TRATTAMENTO
"DATA PROCESSOR"

Art. 4 PARAG. 8 Art. 28

"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" e "che presentino garanzie sufficienti (esperienza, capacità e affidabilità) per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato"

... Il Responsabile del Trattamento

Art. 28

nomina **tramite un contratto** al fine dimostrare che fornisce le *"garanzie sufficienti"*;

E' possibile per un responsabile del trattamento nominare sub-responsabili, previa autorizzazione scritta, specifica o generale, del titolare del trattamento (ES. APPALTO)

il responsabile primario risponde nei confronti del Titolare di eventuali inadempimenti del sub-responsabile

... Il Responsabile del Trattamento

COMPITI

Art. 28

1) **Trattare i dati secondo le istruzioni del Titolare**
2) **Garantire** che gli incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3) **ADOTTARE** le misure richieste dal Regolamento
4) **ASSISTERE** il Titolare con misure tecniche e organizzative adeguate
5) **ASSISTERE** il Titolare nel rispetto degli obblighi delle misure di sicurezza, notifica delle violazioni, valutazione impatto
6) **METTERE** A DISPOSIZIONE del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi
7) **CANCELLA O RESTITUISCE** i dati in suo possesso al termine del suo incarico
8) **INFORMARE TEMPESTIVAMENTE** il Titolare in caso di violazioni del Regolamento

PERSONE AUTORIZZATE AL TRATTAMENTO (*INCARICATI*)

Art. 29

Sono le persone fisiche che effettuano materialmente le operazioni di trattamento dati e operano sotto la diretta AUTORITA' del Titolare o del Responsabile del trattamento con precise istruzioni.

DIRITTI

... L'incaricato

- Formazione
- Istruzioni
- profilo di autorizzazione
- strumenti di lavoro conformi
- Non hanno responsabilità salvo per fatto proprio
- Esercizio diritti degli interessati

IL RESPONSABILE DELLA PROTEZIONE DEI DATI "DATA PROTECTION OFFICER" (DPO)

Art. 37

NUOVA FIGURA

OBBLIGO DI NOMINA

1) Se il trattamento è effettuato da **UN'AUTORITA' PUBBLICA o DA UN ORGANISMO PUBBLICO** *eccetto* le autorità giudiziarie

OBBLIGO DI NOMINA

2) Se le **attività principali** del Titolare o del Responsabile del trattamento **consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**

LARGA SCALA

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

OBBLIGO DI NOMINA

3) Se le **attività principali** del Titolare o del Responsabile del trattamento **consistono** nel trattamento, **su larga scala**, di **categorie particolari di dati o di dati personali relativi a condanne penali o reati**

IN CASO DI GRUPPO DI IMPRESE O SOGGETTI PUBBLICI
NOMINA UNICO DPO

Esempi

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici;

Esempi

- sindacati;
- caf e patronati;
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;
- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

CARATTERISTICHE

Ruolo apicale

Organizzativo

Specializzato

Autonomo

Responsabile

INCARICHI

- **informa e consiglia** (consulenza)
- **sorveglia** l'osservanza del Regolamento, inclusa formazione e sensibilizzazione
- **fornisce parere** in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia l'applicazione
- **coopera** con l'autorità di controllo
- **funge da punto di contatto** per l'autorità di controllo per questioni connesse al trattamento di dati personali;

OBBLIGHI

- **raccoglie informazioni** per identificare i processi di trattamento
- **considera i rischi** inerenti al trattamento, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento stesso
- **gestisce i costi della privacy** (formazione, incaricati, sviluppo e aggiornamento procedure …)
- **analizza la compliance dei processi**
- **informa, segnala e sottopone** questioni e raccomandazioni
- **traccia e documenta la propria attività**

LA VIOLAZIONE DEI DATI "*DATA BREACH*"

Art. 33

In caso di violazione dei dati personali, il Titolare del trattamento **notifica** la violazione **all'autorità di controllo competente** senza ingiustificato ritardo, ove possibile **entro 72 ore dal momento della conoscenza**,
a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.
Se non viene effettuata entro 72 ore, la notifica è corredata di una giustificazione motivata.

OBBLIGO del Titolare di **rendicontare qualsiasi violazione dei dati** personali

COMUNICAZIONE ALL'INTERESSATO

"SENZA INGIUSTIFICATO RITARDO"

con LINGUAGGIO SEMPLICE E CHIARO

CONTENUTO MINIMO DELLA NOTIFICA "*DATA BREACH*"

a) DESCRIZIONE natura della violazione, le categorie violate, il numero di interessati, le circostanze,

b) Il nome e le coordinate di contatto del DPO.

c) Descrizione delle probabili conseguenze della violazione.

d) Descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione.

LE INFORMATIVE
(art. 13 e art. 14 del Regolamento UE)

DIFFERENZE DAL PASSATO ?

SEMPRE RUOLO FONDAMENTALE DELL'INFORMATIVA

ELEMENTI AGGIUNTIVI E DETTAGLIATI

TIPOLOGIE E TEMPI

1) i dati PERSONALI siano RACCOLTI presso L'INTERESSATO (ex art. 13)

→ **l'informativa deve essere fornita all'interessato PRIMA di effettuare la raccolta dei dati**

2) I dati PERSONALI NON siano stati OTTENUTI presso L'INTERESSATO (ex art. 14)

→ **l'informativa deve essere fornita entro *un termine ragionevole* MAX 1 mese dalla raccolta del dato, oppure al momento della comunicazione dei dati a terzi o all'interessato (NON della registrazione)**

CONTENUTO DELL'INFORMATIVA

1) dati di contatto del Responsabile del Trattamento e/o del DPO, ove esistente,
2) la base giuridica del trattamento,
3) **l'interesse legittimo** perseguito dal Titolare o da terzi;
4) I diritti dell'interessato:
   - ✓ *Il diritto di accesso ai dati (art. 15)*
   - ✓ *Il diritto di rettifica (art. 16)*
   - ✓ *Il diritto di cancellazione (c.d. "diritto all'oblio" art. 17)*
   - ✓ *il diritto di presentare un reclamo all'autorità di controllo.*
   - ✓ *Il diritto alla portabilità dei dati (art. 20)*
   - ✓ *Il diritto di revocare il consenso in qualsiasi momento*
5) il periodo di conservazione dei dati,
6) La fonte da cui hanno origine i dati personali
7) Le categorie dei dati personali oggetto del trattamento

CONSIDERANDO 47 del GDPR
legittimo interesse del titolare deve innanzitutto tenersi conto delle *"ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento*

FORMA

- **concisa**, **trasparente**, **intelligibile** e **facilmente accessibile**;
- **linguaggio chiaro e semplice**,
- **informative idonee** per i minori (*rif. considerando 58*).

in linea di principio

scritta e preferibilmente in formato elettronico

può essere fornita anche oralmente (art. 12, paragrafo 1).

Utilizzo di ICONE STANDARDIZZATE (art. 12 parag. 7)

ESONERO DELL'INFORMATIVA

se l'interessato **dispone già dell'informazione**

se la registrazione o la comunicazione dei dati personali **sono previste per legge**

si rivela impossibile o richiederebbe uno sforzo sproporzionato (per trattamenti ai fini statistici, o ricerca storica o scientifica o di pubblico interesse)

obbligo DEL SEGRETO PROFESSIONALE disciplinato dal diritto dell'Unione Europea o dagli Stati membri (ART. 14 PARAG. 5 lett. d))

nei casi indicati nell'art. 23 parag. 1 "LIMITAZIONI"
attività volte a prevenire, indagare, accertare e perseguire violazioni del CODICE DEONTOLOGICO degli Ordini o Albi PROFESSIONALI;

la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali

esecuzione delle azioni civili (*Es. Pignoramento di un quinto dello stipendio*)

ESEMPIO INFORMATIVA PER I CLIENTI

I dati personali del Cliente sono utilizzati da STUDIO GEOM. MARIO ROSSI, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:

- **Cartacei**
- **Informatici (software gestionali, contabili, ecc.)**
- **Telematici**

con le seguenti finalità:

- ❑ **erogazione dei servizi richiesti dal Cliente o disponibili su portali gestiti da Enti Pubblici/società private nonché conclusione del contratto di cui è parte l'interessato;**
- ❑ **fini amministrativi e contabili correlati ai contratti professionali;**
- ❑ **gestione della clientela e fornitori**

L'eventuale rifiuto nel consentire il trattamento dei dati comporta l'impossibilità di usufruire del servizio richiesto dall'utente.

ESEMPIO INFORMATIVA PER I CLIENTI

Fatto salvo esplicito diniego da parte dell'interessato, i dati dell'utente saranno trattati anche per le seguenti finalità:

- invio di proposte e di comunicazioni commerciali a mezzo posta elettronica o SMS o fax, da parte sia di STUDIO GEOM. MARIO ROSSI e sia di società partner (*indicare nominativi se presenti*);

❑ **accetta non accetta**

- news letter , circolari informative ecc…. ;

❑ **accetta non accetta**

BASE GIURIDICA

Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.

Lo STUDIO GEOM. MARIO ROSSI tratta i dati facoltativi del Cliente in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di interessati:

Consulenti; Contabili ed amministrativi; Fornitori, Istituti di credito, Enti Pubblici o privati …..

ESEMPIO INFORMATIVA PER I CLIENTI

PERIODO DI CONSERVAZIONE

I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento del rapporto consulenziale e contabile.

I dati di chi non usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con il Titolare o suoi collaboratori dello Studio, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di consulenza.

DIRITTI DELL'INTERESSATO

Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:

- **richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso);**
- **conoscerne l'origine;**
- **riceverne comunicazione intelligibile;**
- **avere informazioni circa la logica, le modalità e le finalità del trattamento;**
- **richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti;**
- **nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;**
- **il diritto di presentare un reclamo all'Autorità di controllo.**

ESEMPIO INFORMATIVA PER I CLIENTI

Le richieste vanno rivolte al Titolare del trattamento.
Titolare del trattamento dei Suoi dati personali è GEOM. MARIO ROSSI con sede in Reggio Emilia via _____.
Lo scrivente Studio ha nominato quale DPO (Data Protection Officer) il/la Sig./Sig.ra ..... che può essere contattato al seguente indirizzo email: ……

Informazioni sui Cookies
Cosa sono i cookies
Cookie tecnici
Cookie di profilazione
Cookie di terze parti
Tipologie di cookie utilizzati dal nostro sito
Gestione dei cookie
Plugin Social Network
La presente privacy policy può subire modifiche nel tempo – anche connesse all'eventuale entrata in vigore di nuove normative di settore, all'aggiornamento o erogazione di nuovi servizi ovvero ad intervenute innovazioni tecnologiche – per cui l'utente/visitatore è invitato a consultare periodicamente questa *pagina* (*inserire link alla eventuale pagina del sito*).

IL CONSENSO
(artt. 7, 8 e 9 del Regolamento UE)

"inequivocabile"
(*considerando 32 e articolo 7*)

È liberamente espresso

Specifico per il tipo di trattamento

informato

No al consenso tacito o passivo

... il Consenso

Considerando 171

"qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, ***non occorre che l'interessato presti nuovamente il suo consenso****, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento …"*

OBBLIGO DEL CONSENSO

- Il modello utilizzato per la raccolta **non rispetta il requisito di inequivocabilità**
- Il titolare del trattamento **ha considerato come consenso il silenzio o l'inattività dell'interessato**,
- il consenso **sia richiesto solamente per una delle diverse finalità del trattamento** dei dati;
- La formula del consenso **non è chiaramente distinguibile** dalle altre clausole del contratto
- nella formula del consenso **mancano degli elementi => non è comprensibile**
- La formula del consenso **non utilizza un linguaggio semplice e chiaro;**
- Non è espresso che **il consenso possa essere revocato in modo incondizionato** né sono indicate le modalità in cui tale revoca possa avvenire;
- **Non sono indicate l'identità** del titolare del trattamento dei dati **e le finalità** del trattamento.

ATTENZIONE

AL RILASCIO DI LISTE DI DATI PERSONALI, A SOGGETTI TERZI

SPONSOR

CONSENSO FACOLTATIVO

- **ESECUZIONE DI UN CONTRATTO già in essere**
- **DATI PROVENIENTI DA PUBBLICI REGISTRI, ELENCHI, ATTI o DOCUMENTI CONOSCIBILI DA CHIUNQUE**
- **FINALITA' AMMINISTRATIVE E CONTABILI**
- **Per adempiere ad un OBBLIGO LEGALE**
- **per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica**
- **per la gestione del rapporto di lavoro**
- **per far valere un diritto in sede giudiziaria**

REGISTRI DELLE ATTIVITA' DEL TRATTAMENTO

(art. 30 del Regolamento UE)

I SOGGETTI OBBLIGATI

CONTENUTO DEL REGISTRO

REGISTRI DELLE ATTIVITA' DEL TRATTAMENTO
(art. 30 del Regolamento UE)

SOGGETTI OBBLIGATI

IMPRESE O ASSOCIAZIONI CON PIU' DI 250 DIPENDENTI

TRATTAMENTI CON RISCHIO PER I DIRITTI E LA LIBERTA' DELLE PERSONE

TRATTAMENTO DEI DATI NON OCCASIONALE

CATEGORIA PARTICOLARE DI DATI (art. 9)

DATI GIUDIZIARI (art. 10)

CONTENUTO DEL REGISTRO DEI TRATTAMENTI

a) Nome e coordinate del Titolare,co-responsabile, incaricati, Rappresentante, DPO
b) Le finalità del trattamento.
c) Tipo di dati trattati
d) Categoria di interessati e categoria dati.
e) Categoria di destinatari dei dati.
f) Rilascio informativa e consenso
g) Frequenza trattamento
h) I trasferimenti dei dati ai Paesi Terzi o organizzazione internazionale.
i) Modalità di elaborazione dati
j) I termini ultimi per la cancellazione dei dati. NOVITA'
k) Valutazione del rischio
l) Una descrizione generale delle **misure di sicurezza tecniche ed organizzative**.

LE MISURE DI SICUREZZA
(art. 32 del Regolamento UE)

SICUREZZA DEL TRATTAMENTO

- Cifratura e pseudo-nimizzazione dei dati personali.
- Capacità di assicurare la continua riservatezza, integrità, disponibilità dei sistemi.
- Capacità di ripristino tempestivo dei dati in caso di incidente fisico o tecnico.
- Una procedura per provare /verificare/ valutare l'efficacia delle misure scelte
- Codici di condotta o certificazione (**elementi per dimostrare la conformità** ai requisiti delle misure di sicurezza).

COME SI VALUTA L'ADEGUATEZZA ?

si tiene conto in special modo :

1) Rischio significativi per i diritti e la libertà fondamentale della persona

- se il trattamento comporta discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo
- Impedimento dell'esercizio del controllo dei propri dati personali;
- se sono trattati dati personali "particolari";
- in caso di valutazione del rendimento professionale, della situazione economica, della salute, delle preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali
- Dati di minori
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Rischio distruzione,
Rischio perdita,
Rischio modifica,
Rischio divulgazione non autorizzata
Rischio accesso, in modo accidentale o illegale

GARANTIRE I DIRITTI DEGLI INTERESSATI FIN DALLA PROGETTAZIONE (privacy by design)

OBBLIGO di

mettere in atto misure tecniche ed organizzative adeguate e **misure volte ad attuare la minimizzazione del trattamento** tenuto conto:

- dello stato dell'arte
- dei costi di attuazione,
- della natura,
- del contesto
- del campo di applicazione
- delle finalità del trattamento
- **probabilità / gravità del rischio** per i diritti e le libertà delle persone fisiche

Valutazione oggettiva (*Considerando 76*)

GARANTIRE PER IMPOSTAZIONE PREDEFINITA (privacy by default)

OBBLIGO di
mettere in atto misure tecniche ed organizzative adeguate affinché vengano trattati, **per impostazione predefinita**, **solo dati necessari per ogni specifica finalità**

- Quantità di dati raccolti
- portata del trattamento
- periodo di conservazione
- accessibilità

VALUTAZIONE DEL RISCHIO

L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento** (P) ed alle **conseguenze di tale evento** (C).

LR = P X C

LR = livello di rischio P = probabilità di accadimento C = conseguenze

PROBABILITA' DELL'EVENTO	
1	IMPROBABILE
2	POCO PROBABILE
3	PROBABILE
4	MOLTO PROBABILE
5	QUASI CERTO

CONSEGUENZE	
1	TRASCURABILI
2	MARGINALI
3	LIMITATE
4	GRAVI
5	GRAVISSIME

VALUTAZIONE DEL RISCHIO

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

P						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		C				

ENTITA' RISCHIO	VALORE DI RIFERIMENTO
ACCETTABILE	$(1 \leq LR \leq 3)$
MEDIO - BASSO	$(4 \leq LR \leq 6)$
RILEVANTE	$(8 \leq LR \leq 12)$
ALTO	$(15 \leq LR \leq 25)$

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

(art. 35 del Regolamento)

REGOLA SPECIFICA

a) Una valutazione SISTEMATICA E GLOBALE di aspetti personali relativi a persone fisiche, basata su trattamento automatizzato, compresa profilazione.

ESEMPI OSPEDALE, videosorveglianza per il controllo del traffico stradale

b) Il trattamento su larga scala di dati sensibili o dati giudiziari.

ESEMPI Società creditizie , società assicurative

c) La sorveglianza sistematica di una zona accessibile al pubblico su larga scala.

ESEMPI Comune, videosorveglianza nel Centro Commerciale

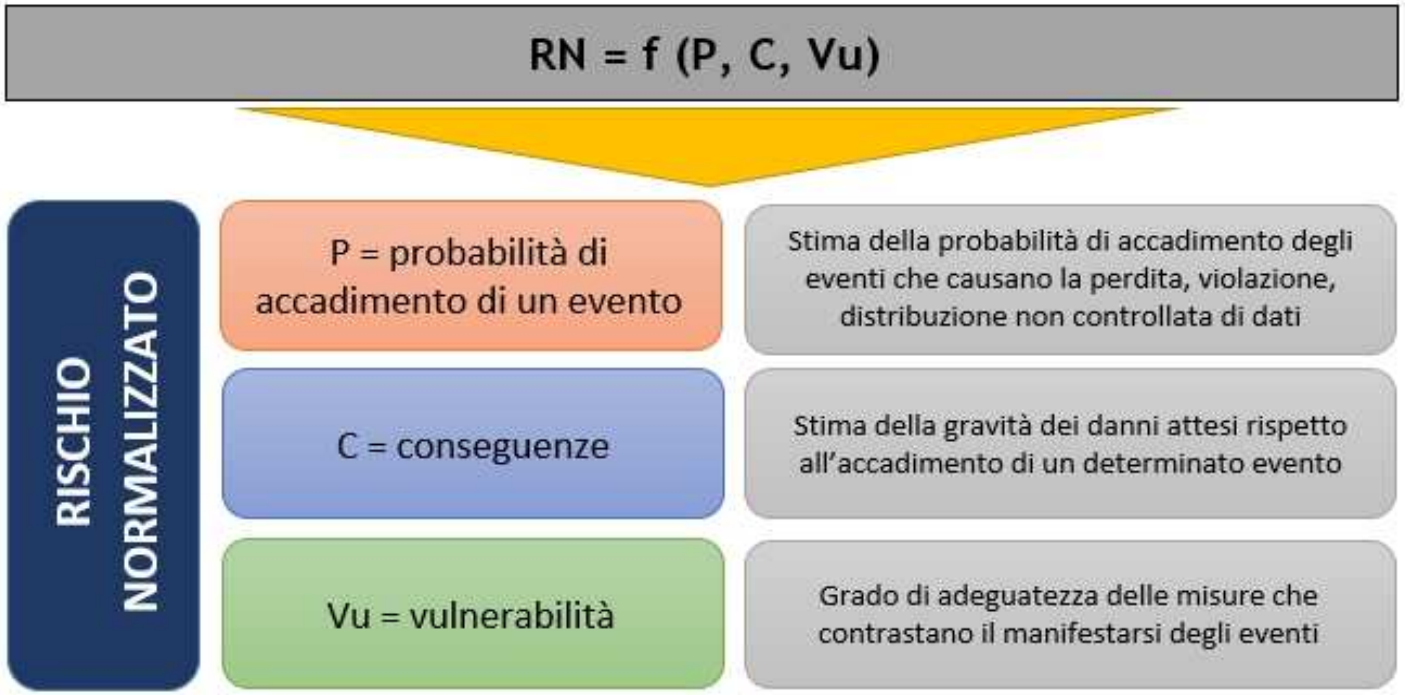
NO VALUTAZIONE D'IMPATTO

singolo medico / avvocato

Rivista online che utilizza una mailing list

CONTENUTO DELLA VALUTAZIONE D'IMPATTO

Il rischio viene calcolato in funzione dei 3 fattori seguenti:



In prima battuta viene ricavato il **rischio intrinseco Ri**, considerando tutti i possibili **pericoli e i rischi**.:

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	·Perdita ·Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	·Perdita ·Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	·Perdita ·Distruzione non autorizzata ·Modifica non autorizzata ·Divulgazione non autorizzata ·Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	·Perdita ·Distruzione non autorizzata ·Modifica non autorizzata ·Divulgazione non autorizzata ·Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	·Perdita ·Distruzione non autorizzata ·Modifica non autorizzata ·Divulgazione non autorizzata ·Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	·Perdita ·Distruzione non autorizzata ·Modifica non autorizzata ·Divulgazione non autorizzata ·Accesso dati non autorizzato

rischio intrinseco Ri= P x C in base agli indici numerici assegnati ad entrambi i fattori.:

PROBABILITA' DELL'EVENTO	
1	IMPROBABILE
2	POCO PROBABILE
3	PROBABILE
4	QUASI CERTO

CONSEGUENZE	
1	TRASCURABILI
2	MARGINALI
3	LIMITATE
4	GRAVI

P					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		C			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

Per ricavare il **Rischio Normalizzato RN**, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

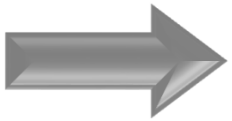
Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con **il valore peggiore assegnato** (1) alle misure di sicurezza relativamente a quel rischio.

V					
	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,2	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

CONSULTAZIONE PREVENTIVA
(art. 36 del Regolamento UE)

In caso di assenza di misure da adottare per ridurre il rischio elevato, il Titolare del trattamento consulta preventivamente l'autorità di controllo che rilascia parere scritto entro 8 settimane dalla richiesta.



Simile alla Verifica preliminare
Art. 17 Codice Privacy

CONTENUTO DELLA COMUNICAZIONE ALL'AUTORITA' DI CONTROLLO

- Le responsabilità del titolare del trattamento, dei contitolari, dei responsabili.
- Le finalità ed i mezzi del trattamento
- Le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati
- I dati di contatto del titolare
- La valutazione d'impatto sulla protezione dei dati.

PROCEDIMENTO

L'Autorità di Controllo VALUTA:

- **se il trattamento descritto è conforme al Regolamento**
- **se il titolare ha identificato ed attenuato il rischio in maniera sufficiente**

In caso di esito negativo della valutazione, l'Autorità fornisce al titolare del trattamento una consulenza per iscritto

CODICI DI CONDOTTA

Il codice di condotta rappresenta uno strumento volontario mediante il quale il Titolare del trattamento dimostra che il trattamento dei dati è stato attuato in conformità al Regolamento.

Diverso dal codice etico

Identifica gli obblighi tra l'impresa e le parti interessate

Obbliga l'impresa al rispetto dei criteri guida indicati

CODICI DI CONDOTTA GIORNALISTI

IKEA si impegna a non utilizzare lavoro minorile nelle sue fasi produttive

PROCEDURA

ELABORARE IL CODICE DI CONDOTTA definendo :

- **La *MISSION* aziendale**
- **Gli OBIETTIVI da raggiungere**
- **Le RESPONSABILITA' DELLA DITTA nei confronti delle parti interessate**

DIVULGARE IL CODICE a tutte le parti interessate (sia interne che esterne all'impresa)

VERIFICARE CHE I PRINCIPI siano rispettati

INDIVIDUARE I COMPORTAMENTI SCORRETTI

ASSEGNARE EVENTUALI SANZIONI

REVISIONARE IL CODICE DI CONDOTTA

GRAZIE PER L'ATTENZIONE !

STUDIO DI CONSULENZA DEL LAVORO

Dott. Luciana Bruno

Via Meuccio Ruini, 74 - 42124 Reggio Emilia

0522 / 27.24.23 – mail: lucianabruno@yahoo.it