privacy officer.pro

PROFESSIONISTI DELLA PRIVACY

STUDIO LEGALE AVVOCATI D'AGOSTINI

GDPR E NUOVO CODICE PRIVACY: ADEMPIMENTI E RESPONSABILITÀ NEL TRATTAMENTO DEI DATI PERSONALI

Prof. Avv. David D'Agostini

7 novembre 2018

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020

UN INVESTIMENTO PER IL TUO FUTURO

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

in rete fvg
seminari per l'innovazione in rete

QUADRO NORMATIVO

PRIMA

Unione europea:

- Direttiva 1995/46/CE

Italia:

- d.lgs. 30.06.2003 n. 196 (Codice privacy)

ADESSO

Unione europea:

- Regolamento (UE) 2016/679 GDPR

Italia:

- d.lgs. 30.06.2003 n. 196 (modificato dal d.lgs. 101/18)

DATO PERSONALE

Qualsiasi informazione che riguardi una **persona fisica** identificata o identificabile.

È 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.

DATI PERSONALI “SENSIBILI”

Categorie particolari di dati personali (art. 9 GDPR) che riguardano:

- lo stato di salute
- i dati genetici o biometrici
- la vita sessuale o l'orientamento sessuale
- l’origine razziale o etnica
- le convinzioni religiose o filosofiche
- le opinioni politiche
- l’adesione a organizzazioni sindacali

I SOGGETTI

PRIMA

- Interessato
- Titolare del trattamento
- Responsabile del trattam.
- Incaricato del trattamento

======

ADESSO

- Interessato
- Titolare del trattamento
- Responsabile del trattam.

=======*

- Data Protection Officer

(Responsabile della Protezione dei Dati)

*Persona autorizzata al trattamento sotto l'autorità del titolare

I SOGGETTI

- **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento

- **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

RESPONSABILE DEL TRATTAMENTO

Contratto tra Titolare e Responsabile prevede, in particolare, che quest'ultimo:

a) tratti i dati personali soltanto su istruzione documentata del titolare;

b) garantisca che le persone autorizzate al trattamento dei dati personali (incaricati) si siano impegnate alla riservatezza;

c) adotti tutte le adeguate misure di sicurezza;

d) sia eventualmente autorizzato dal Titolare a ricorrere a un Subresponsabile del trattamento;

RESPONSABILE DEL TRATTAMENTO

e) assista il Titolare al fine di soddisfare le richieste per l'esercizio dei diritti dell'interessato;

f) assista il Titolare nel garantire il rispetto degli obblighi in materia di sicurezza;

g) su scelta del Titolare, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento;

h) metta a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto del GDPR e consenta le attività di revisione, comprese le ispezioni, realizzate dal Titolare.

DATA PROTECION OFFICER

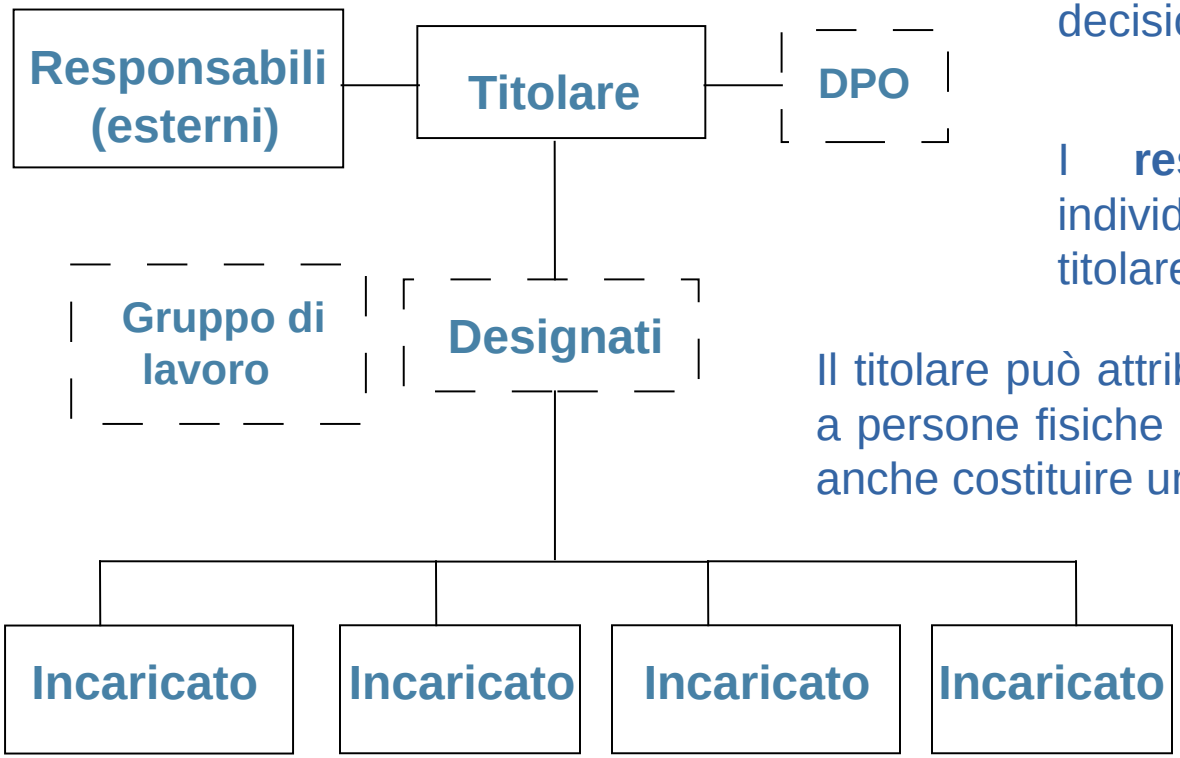
Il **Responsabile della Protezione dei Dati** (RPD) o **Data Protection Officer** (DPO) va designato se:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;

b) le attività principali consistono in trattamenti che (per loro natura, ambito di applicazione e/o finalità) richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le attività principali consistono nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e reati.

ORGANIGRAMMA



Il **titolare** è l'entità nel suo complesso che esercita un potere decisionale autonomo.

I **responsabili** (esterni) sono individuati obbligatoriamente dal titolare.

Il titolare può attribuire specifici compiti e funzioni a persone fisiche espressamente **designate** (può anche costituire un "**gruppo di lavoro**").

Con la designazione degli **incaricati** viene individuato l'ambito del trattamento consentito.

Le operazioni del trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare (o del responsabile) attendendosi alle istruzioni impartite.

TO DO LIST - 1° STEP

- Individuare tutti i soggetti del trattamento
- Formalizzare il rapporto con gli incaricati
- Valutare se attribuire specifiche funzioni a soggetti designati
- Stipulare il contratto con i responsabili (esterni)
- Nominare il DPO (se sussiste l'obbligo o se ritenuto opportuno)

e comunicarne i dati di contatto al Garante

REGISTRO DEI TRATTAMENTI

Il Titolare del trattamento compila un registro delle attività di trattamento svolte (che, su richiesta, va messo a disposizione del Garante privacy).

Tale registro contiene le seguenti informazioni:

a) nome e dati di contatto del Titolare del trattamento e del DPO;

b) finalità del trattamento;

c) descrizione delle categorie di interessati e delle categorie di dati personali;

REGISTRO DEI TRATTAMENTI

d) categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) trasferimenti extra UE di dati personali;

f) termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) descrizione generale delle misure di sicurezza tecniche e organizzative.

L’INFORMATIVA

L’informativa agli Interessati va resa:

- in forma concisa
- per iscritto (oralmente su richiesta dell'interessato, purché ne sia comprovata l'identità)
- trasparente
- intellegibile
- facilmente accessibile
- con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori

CONTENUTO

- l'identità e i dati di contatto del titolare del trattamento e dell'eventuale DPO;
- le finalità del trattamento, nonché la base giuridica del trattamento;
- i legittimi interessi perseguiti dal titolare o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;

CONTENUTO

- il periodo di conservazione dei dati ovvero i criteri utilizzati per determinare tale periodo
- l'esistenza dei diritti dell'interessato (accesso, cancellazione, etc.)
- il diritto di proporre reclamo a un'autorità di controllo;
- se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

LICEITÀ DEL TRATTAMENTO

Il trattamento è lecito se:

- l'interessato ha espresso il consenso

...oppure se è necessario:

- all'esecuzione di un contratto
- per obbligo di legge
- per la salvaguardia di interessi vitali
- per un interesse pubblico (P.A.)
- per un legittimo interesse del titolare

CONSENSO

Il trattamento è lecito se l'interessato ha espresso il consenso.

Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

CONSENSO

La richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento (di ciò ne è informato prima); il consenso è revocato con la stessa facilità con cui è accordato.

TO DO LIST - 2° STEP

- Mappare i trattamenti dei dati personali
- Definire i tempi di conservazione
- Redigere il registro dei trattamenti
- Rendere agli interessati l'informativa
- Valutare la base giuridica di ciascun trattamento
- Acquisire il consenso laddove necessario
- Pubblicare i dati di contatto del DPO [se nominato] e comunicarli al Garante

I PRINCIPI DEL GDPR

liceità, correttezza e trasparenza

limitazione della finalità

integrità e riservatezza

PRINCIPI

minimizzazione dei dati

limitazione della conservazione

esattezza e aggiornamento

I “NUOVI” IMPERATIVI

1) Trattare meno dati personali possibile

2) Favorire anonimizzazione, cifratura e pseudonimizzazione dei dati

3) Documentare gli aspetti rilevanti del trattamento (adempimenti, decisioni, valutazioni, etc.)

4) Essere in grado di dimostrare che il trattamento rispetta la normativa

PRIVACY BY DESIGN

Il Titolare, tenendo conto

1) dello **stato dell'arte** e dei **costi di attuazione**,

2) della natura, dell'ambito di applicazione, del contesto e delle finalità del **trattamento**,

3) come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,

mette in atto

misure **tecniche** e **organizzative** adeguate (es. pseudonimizzazione) volte ad attuare in modo efficace i principi di protezione dei dati (es. minimizzazione) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare gli interessati.

PRIVACY BY DEFAULT

Il Titolare mette in atto misure **tecniche** e **organizzative** adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

I DIRITTI DELL'INTERESSATO

- Diritto di accesso
- Diritto di rettifica
- Diritto di cancellazione (“oblio”)
- Diritto di limitazione di trattamento
- Diritto di opposizione

Riscontro entro un mese (prorogabile di due mesi, informando l'interessato della proroga e dei motivi entro il primo mese!)

NUOVA SICUREZZA

Tenuto conto della valutazione del rischio, dell'evoluzione tecnica e dei costi di attuazione, il Titolare mette in atto **misure tecniche e organizzative** adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta:

a) pseudonimizzazione e cifratura dei dati personali

b) capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi

c) capacità di ripristinare tempestivamente disponibilità e accesso

VIOLAZIONE DEI DATI PERSONALI

Data Breach: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Va notificata al Garante privacy entro 72 ore dalla conoscenza e comunicata gli interessati in caso di rischio elevato per i loro diritti.

TO DO LIST - 3° STEP

- Accertare il rispetto dei principi del GDPR
- Applicare la protezione dei dati by design e by default
- Saper gestire le richieste dell'interessato
- Approvare una procedura per il caso di data breach
- Effettuare verifiche periodiche (PDCA)
- Aggiornarsi costantemente (sito internet www.garanteprivacy.it)

RESPONSABILITÀ

Responsabilità civile : Risarcimento dei danni materiali e immateriali

Sanzioni amministrative pecuniarie fino a €20.000.000, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente.

Sanzioni penali (es. trattamento illecito di dati, falsità nelle dichiarazioni al Garante, inosservanza di provvedimenti del Garante)

Prof. Avv. David D’Agostini

studio@avvocatidagostini.it

info@privacyofficer.pro

Via Vittorio Veneto 32 - Udine