Dalla compliance al GDPR come strumento di efficienza. Dal COVID19 alle strategie di marketing.

Webinar

21 Maggio 2020

Avv. Laura Priore

COSA FARE PER ESSERE IN LINEA CON IL *GDPR*?

1° passo: ***check list***

- ✓ Individuare i trattamenti di dati personali oggetto di trattamento e le categorie di soggetti interessati. Che dati tratto? Chi sono i soggetti interessati? (clienti, fornitori, lavoratori, candidati)
- ✓ Adotto misure di sicurezza?
- ✓ Per quanto tempo conservo il dato?
- ✓ A chi trasmetto i dati personali che raccolgo?
- ✓ Individuare i soggetti interessati dal trattamento ed i loro ruoli (chi è il titolare del trattamento? Il responsabile del trattamento? Devo incaricare i miei dipendenti come soggetti autorizzati al trattamento? Devo nominare il *Data Protection Officer*?)

I NUOVI PRINCIPI

Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (Art. 25)

- *Privacy* ***By Design***: sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati.
- *Privacy* ***By Default***: Il titolare del trattamento 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.

IL PRINCIPIO 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 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.

DUE REGOLE FONDAMENTALI

1. Le persone che «collaborano» nel trattamento di dati personali **devono ricevere un'apposita nomina.**

2. Le persone che mi «affidano» i propri dati personali **devono ricevere un'apposita informativa.**

LE NOMINE

- **I soggetti autorizzati al trattamento (ex incaricati): i destinatari interni.**

  Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità, autorizzandole al trattamento. Art. 2-*quaterdecies* Codice della Privacy.

- **I soggetti responsabili del trattamento (art. 28 GDPR): i destinatari esterni.**

  Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico.

QUANDO RILASCIARE L'INFORMATIVA E QUANDO RICHIEDERE IL CONSENSO?

2° passo: adeguamento informative e consensi

- Non tutte le volte che devo rilasciare l'informativa devo richiedere il consenso, **si tratta di due «binari» distinti.**
- I contenuti dell'informativa sono **elencati in modo tassativo** nell'art. 13 del GDPR e in parte sono più ampi rispetto al Codice.
- L'informativa deve essere fornita all'interessato **prima di effettuare la raccolta dei dati.**

CONTENUTO DELL'INFORMATIVA

1. Il **titolare** ed i suoi dati di contatto.
2. Il ***Data Protection Officer*** (qualora presente).
3. Le **finalità** del trattamento e la base giuridica.
4. Gli eventuali **destinatari.**
5. L'intenzione di **trasferire dati extra UE.**
6. Il **periodo di conservazione** dei dati.
7. I **diritti** dell'interessato.
8. L'esistenza di un **processo decisionale automatizzato** (compresa la profilazione e la logica utilizzata).

LE BASI GIURIDICHE DEL TRATTAMENTO

- Ogni trattamento deve trovare fondamento in **un'idonea base giuridica**.
- **Il consenso non è l'unica** base giuridica.
- Il regolamento **elenca le basi giuridiche** sia per i «dati comuni» sia per i «dati particolari».

6 BASI GIURIDICHE PER I DATI COMUNI

1. Il **Consenso.**
2. Esecuzione di un **contratto** o di misure precontrattuali.
3. L' **obbligo legale**.
4. Salvaguardia degli **interessi vitali**.
5. L'esecuzione di un compito di **interesse pubblico**.
6. Il **legittimo interesse** 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.

10 BASI GIURIDICHE PER I DATI PARTICOLARI

È vietato trattare:

- **dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale;**
- **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.**

10 BASI GIURIDICHE PER I DATI PARTICOLARI

Il divieto non si applica se si verifica uno dei seguenti casi:

1. Il **Consenso.**
2. Per assolvere gli obblighi in materia di **diritto del lavoro**.
3. Per tutelare un **interesse vitale.**
4. Trattamento effettuato da una **fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità politiche, filosofiche, religiose o sindacali
5. Dati personali **resi manifestamente pubblici** dall'interessato.
6. Per accertare, esercitare o difendere un **diritto in sede giudiziaria**.
7. Per motivi di **interesse pubblico**.
8. Per finalità di **medicina preventiva o di medicina del lavoro**.
9. Per motivi di interesse pubblico nel settore della **sanità pubblica**.
10. Per fini di **archiviazione, di ricerca scientifica o storica o a fini statistici**.

GLI ALTRI ADEMPIMENTI DEL GDPR

3° passo: adeguamento procedure interne e adozione nuovi strumenti previsti dal GDPR.

- Il registro dei trattamenti (art. 30 GDPR)
- La valutazione di impatto sulla protezione dei dati (art. 35 GDPR)
- La procedura di *data breach* (artt. 33 e 34 GDPR)

IL REGISTRO DEI TRATTAMENTI

- L'art. 30 del Regolamento prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.
- E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30) relative alle operazioni di trattamento svolte dal titolare.
- Costituisce **uno dei principali elementi di *accountability*** del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.
- Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (Art. 35)

- È una procedura che va eseguita quando un tipo di trattamento, allorché preveda **in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- Contiene una **descrizione sistematica dei trattamenti previsti e delle finalità** del trattamento, una **valutazione della necessità e proporzionalità** dei trattamenti in relazione alle finalità, una **valutazione dei rischi** per i diritti e le libertà degli interessati e **le misure previste per affrontare i rischi.**
- Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (*accountability*) dei titolari nei confronti dei trattamenti da questi effettuati.

LA PROCEDURA DI *DATA BREACH*

- Una **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.
- Il titolare del trattamento **senza ingiustificato ritardo** e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali **a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.**
- Inoltre, **se la violazione comporta un rischio elevato per i diritti delle persone**, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.
- Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta tutte le violazioni dei dati personali.**

CASI SPECIFICI:
I TRATTAMENTI NELL'AMBITO DELL'EMERGENZA SANITARIA E PER IL *MARKETING*

Tutti gli strumenti esaminati (*Privacy By Design* e *Privacy By Default*, le nomine, le informative, le procedure interne) vanno adeguate ed implementate per ogni nuovo trattamento effettuato dal titolare del trattamento secondo il principio dell'*accountability*.

I TRATTAMENTI NELL'AMBITO DELL'EMERGENZA SANITARIA

Nell'ambito della gestione dell'emergenza sanitaria da Covid 19 i profili *privacy* riguardano:

1. La **valutazione di impatto** sui nuovi trattamenti predisposti (per esempio nell'ambito dello *smart working*).
2. L'aggiornamento delle **informative** per la rilevazione dello stato di salute dei dipendenti e per le nuove modalità lavorative.
3. L'aggiornamento delle **nomine** e delle **istruzioni operative**.
4. La predisposizione di **procedure interne** per la rilevazione dello stato di salute dei dipendenti.
5. Il rinforzamento della **procedura di *data breach*** per le tecnologie utilizzate e per i dati trattati.

LA BASE GIURIDICA DEL TRATTAMENTO

- **Che tipo di dati sono trattati**? Dati comuni e dati particolari. Solo i dati necessari.
- **Chi può trattare questi dati**? I soggetti pubblici e privati secondo il Protocollo di condivisione della regolamentazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid 19 negli ambienti di lavoro del 14.03.2020 aggiornato il 24.04.2020.
- **Devo Rilasciare un'idonea informativa**? Sì, la finalità del trattamento è la prevenzione dal contagio Covid 19.
- **Qual è la base giuridica**? La base giuridica è l'implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. 1 n. 7 lett. d del DPCM 11.03.2020 e successive modifiche.
- **Qual è la durata**? Si può fare riferimento al termine dello stato di emergenza.

MARKETING

Il rispetto della *privacy* va considerato non solo un requisito di legge, ma anche un **necessario attributo qualitativo** per le tecniche di comunicazione e fidelizzazione commerciale moderne, come un "valore" in termini di lealtà e trasparenza del messaggio pubblicitario stesso.

REGOLE BASE DELLA *PRIVACY* PER LE ATTIVITÀ DI *MARKETING*

1. **Principio del controllo dei propri dati personali**:
   il soggetto interessato deve essere previamente informato circa l'utilizzo dei propri dati per finalità di marketing di terzi come le aziende e deve essere in grado di accettare in maniera espressa o al contrario di rifiutare tale utilizzo, mantenendo un ragionevole controllo anche successivamente con la possibilità di revocare il proprio consenso e ottenere la cancellazione dei propri dati in modo agevole e tempestivo.

2. **Principio del *marketing* «responsabile»:**
   utilizzare i dati a fini commerciali costituisce in generale una finalità legittima e consentita ma deve essere una attività improntata alle trasparenza e alla correttezza anche nelle forme di interazione digitale evitando pratiche commerciali sleali e scorrette.

LA BASE GIURIDICA

1. E' necessario **prima** individuare la strategia di *marketing* e **successivamente** impostare **il sistema di regole** per il rispetto della *privacy (*telefonate con o senza operatore, utilizzo del sito internet, *spam*, *soft-spam*, carte fedeltà). Ciò risponde ai *privacy by design* e *by default* e principio di *accountability*.
2. Le **condizioni di liceità del trattamento** di dati personali nelle attività di marketing
   - consenso dell'interessato;
   - interesse legittimo prevalente del Titolare (*soft spam*).