webinar CALYPSO Privacy

GDPR

(General Data Protection Regulation)

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

Sommario

Cosa affronteremo in questo webinar?

1. La nuova normativa e la sua Applicazione
2. Le Nuove Figure
3. Rischi, Responsabilità e Sanzioni
4. Da dove partire
5. La soluzione Calypso

Normativa

OGGETTO e FINALITA' del GDPR (Art. 1)

Il GDPR è una norma Europea che ha come finalità la protezione e salvaguardia dei dati personali dei cittadini europei, e si applica anche a imprese ed enti, organizzazioni in generale, con sede legale fuori dall'UE che trattino dati personali di residenti nell'Unione Europea

Normativa

TARGET

Il GDPR è rivolto ad Aziende, Enti pubblici, Professionisti i quali, nell'esercizio delle proprie attività trattino a vario titolo dati di privati cittadini della UE

TIMELINE

Il 24/05/2016 è entrato in vigore il GDPR e dal **25/05/2018** verrà applicato in tutti i Paesi dell'UE

Normativa

INOSSERVANZA

La mancata osservazione della norma comporta sanzioni fino a 20 Milioni di € o il 4% del Fatturato annuo Globale.

GDPR

(General Data Protection Regulation)

La nuova normativa e la sua Applicazione

Il DATO PERSONALE (Art. 4)

La definizione di dato Personale, è piuttosto estesa e lo si può capire vedendone l'enunciazione :

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») **(C26, C27, C30)**

salvo una successiva ulteriore classificazione tra Dati Genetici, Biometrici, Relativi alla Salute.

Normativa

L' INTERESSATO (Art. 4)

E' una persona fisica, il cardine intorno al quale, o meglio intorno ai suoi diritti, ruota tutta la nuova normativa.

…una persona fisica identificata o identificabile; 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

Normativa

IL TRATTAMENTO (Art. 4)

Questo è il principale onere a nostro carico, ed è determinato dalla nostra politica della Privacy.

«.. qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;»

Normativa

L'INFORMATIVA (Artt. 13,14)

L'informativa, fa parte del principio di trasparenza con cui l'Azienda tratta i dati dell'Interessato. Anche se a livelli differenti (Dati comuni o Rilevanti), l'informativa deve essere chiara, e deve essere fornita nei tempi e nei modi adeguati.

L'INFORMATIVA (Artt. 13,14)

Il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

L'INFORMATIVA (Artt. 13,14)

Tempi dell'informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON**della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

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

Normativa

L'INFORMATIVA (Artt. 13,14)

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

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

LICEITA' (Art.6)

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

Normativa

LICEITA' (Art.6)

a) l'**interessato** ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il **titolare del trattamento**;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'**interessato è un minore**

L'APPLICAZIONE (Art. 24)

Nel GDPR, è data ampia discrezionalità al titolare e responsabili dei trattamenti, nel decidere le policy più adeguate e sostenibili nella tutela dei dati da parte delle Aziende. Come contropartita viene richiesto però di dimostrare quali siano state le motivazioni che hanno portato a determinare le decisioni prese in fatto di tutela dei dati.

Così non era per la vecchia privacy (Misure Minime).

L'APPLICAZIONE (Art. 24)

Questo nuovo approccio, tradotto impropriamente come «responsabilità», nel GDPR è denominato ACCOUNTABILITY. La traduzione più corretta, anche se poco pratica, potrebbe essere quella di «rendicontazione» (già presente nel settore pubblico).

L'accountability coinvolge aspetti quali l'affidabilità e la competenza aziendale nella gestione dei dati personali determinando un vero e proprio MODELLO DI GESTIONE dei dati aziendali e non solo una norma da rispettare.

ACCOUNTABILITY (Art. 24)

Il GDPR recepisce tale principio e prevede che, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento.

ACCOUNTABILITY (Art. 24)

Dette misure devono essere riesaminate e aggiornate qualora necessario e, se ciò è adeguato rispetto alle attività di trattamento, tali misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

PRINCIPI

I principi di Privacy by Design e by Default (art.25) richiedono che la protezione dei dati faccia parte del progetto di sviluppo dei processi aziendali per prodotti e servizi. Significa pensare già al momento della progettazione di un flusso, all'implicazione che lo stesso avrà nella gestione dei dati della privacy.

GDPR

(General Data Protection Regulation)

Nuove Figure

PRINCIPI

Oltre ad una più estesa definizione di INTERESSATO, nonché la maggior tutela a cui i dati di quest'ultimo sono soggetti, la norma introduce nuovi ruoli e nuovi soggetti che, a vario titolo, sono coinvolti nella gestione dei TRATTAMENTI

TITOLARE DEL TRATTAMENTO (Art. 4)

La figura del titolare del trattamento è centrale, in quanto determina le finalità e i mezzi del trattamento; è colui che definisce le linee guida per la gestione della Privacy della propria Azienda/Ente. Ha potere decisionale e deve svolgere attività di controllo sul trattamento complessivo.

TITOLARE DEL TRATTAMENTO (Art. 4)

- Può nominare uno o più responsabili od uno o più incaricati del trattamento dei dati.
- Tiene il Registro delle Attività del Trattamento del Titolare. *(superiore a 250 addetti ma è buona prassi la sua compilazione)*
- Un Trattamento può prevedere anche in Contitolare

RESPONSABILE DEL TRATTAMENTO (Art. 4)

Tratta i dati personali per conto del Titolare del Trattamento.

E' nominato dal Titolare del Trattamento e può avere facoltà di nomina di altri Responsabili.

DPO (Art. 37)

Il Data Protection Officer (DPO) è designato dal Titolare e dal Responsabile solo in specifici casi; le qualità professionali e la conoscenza della normativa, consentono al DPO la completa governance dei processi relativi alla Privacy.

Forma le persone, sorveglia l'osservanza della Norma, coopera con le autorità di controllo e valuta i rischi.

GDPR

(General Data Protection Regulation)

Rischi, Responsabilità e Sanzioni

RISCHI PER L'INTERESSATO (considerando 75)

I rischi nei quali l'INTERESSATO potrebbe incorrere in caso di cattiva gestione nel trattamento dei propri dati sono:

- danni fisici,
- danni materiali,
- discriminazione,
- furto d'identità,
- perdite finanziarie,
- pregiudizio alla reputazione,
- perdita di riservatezza,
- danni economici,
- danni sociali.

ESERCIZIO DI ATTIVITA PERICOLOSE(art.2050 CC)

Considerando quindi la gestione dei dati Aziendali, un'attività pericolosa, ci si può rifare al Codice Civile, citando :

«Chiunque cagiona danno ad altri nello svolgimento di un'**attività pericolosa**, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.»

(considerando 75) I rischi per i diritti e le libertà delle **persone fisiche**, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare 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; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

(considerando 76) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

RISCHI PER L'AZIENDA

L'INTERESSATO, nel caso ritenga che i propri diritti siano stati violati, potrebbe proporre un ricorso giurisdizionale nei confronti del titolare o rappresentante del trattamento, dinnanzi alle autorità giurisdizionali dello Stato in cui risiede. (art.78,79).

La richiesta di risarcimento danni è inoltre contemplata all'art.82,

SANZIONI

Il regime sanzionatorio, per cui è ancora rilevante il vecchio codice della privacy, (*) prevede una scala di sanzioni che parte dall'ammonimento fino ad arrivare nei casi più «disperati» al 4% del fatturato o 20 Milioni di Euro.

GDPR

(General Data Protection Regulation)

Da dove partire

Partenza

KICK-OFF

Il 25 Maggio è l'inizio di un percorso di compliance alla nuova Normativa. Non è la deadline bensì l'inizio di un nuovo modello dinamico di gestione dei dati e di loro integrazione nei processi Aziendali.

Partenza

COSA FARE?

Per essere compliant è necessario capire quanto i nostri processi impattino sulla gestione dei dati, non dal punto di vista dell'Azienda ma da quello dell'interessato.

- Capiamo quali dati trattiamo, quali tratteniamo, per quanto li tratteniamo e perché, come li gestiamo e chi vi ha accesso.

Partenza

COSA FARE?

- Facciamo chiarezza all'interno della nostra struttura per capire quali flussi hanno la necessità di determinare dei TRATTAMENTI.
- Sulla base di questo, determiniamo la **nostra politica di Trasparenza** nei confronti degli interessati, perché è questa che ci tutela nel momento in cui si dovessero evidenziare criticità.
- Coinvolgiamo i Responsabili, Titolari, i DPO e gli addetti nel processo di responsabilizzazione, determinando un modello comportamentale sostenibile.

Partenza

COSA FARE?

- Formiamo adeguatamente le figure (come richiesto dal GDPR).

- Interveniamo sulle aree a maggior visibilità quali :

- ❑ sito web Aziendale
- ❑ Profili social
- ❑ Cookies
- ❑ Sistemi di Profilazione
- ❑ Newsletter
- ❑ Posta Elettronica
- ❑ Backup
- ❑ Cloud

Partenza

COSA FARE?

Il Regolamento, fortunatamente non ci vincola con strumenti, e quindi possiamo decidere come agire ma :

PRENDIAMO SEMPRE IN CONSIDERAZIONE L'INTERESSATO ED I SUOI DIRITTI E FACCIAMO SI DI CONOSCERE LE LINEE GUIDA CHE IL GDPR CI FORNISCE.

GDPR

(General Data Protection Regulation)

Calypso Privacy