REG. EU 2016/679

1) Impatto normativo

2) Come fare per mettersi in regola

3) Sanzioni

1. Novità normative del Reg. EU 2016/679

- A) Fondamenti di liceità del trattamento dati
- B) Informativa
- C) Diritti degli interessato

1. Novità normative del Reg. EU 2016/679

D) Titolare, responsabile, incaricato del trattamento

E) Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili

F) Trasferimenti di dati verso paesi terzi e organismi internazionali

A. Fondamenti di liceità del trattamento

CONSENSO

- Esplicito (per dati sensibili)
- Non necessariamente scritto, ma onere prova a carico titolare
- I minori di anni 16 possono fornirlo

INTERESSE VITALE DI UN TERZO

- Può essere utilizzato solo in via residuale

INTERESSE LEGITTIMO PREVALENTE DEL TITOLARE O DI UN TERZO

- Il bilanciamento spetta al titolare

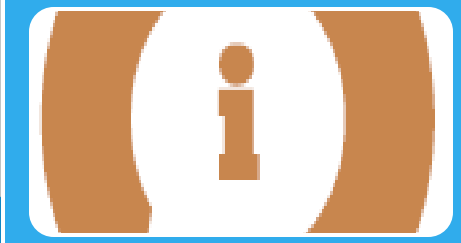
B. Informativa

CONTENUTI DELL'INFORMATIVA

- Indicati in modo tassativo nell'art. 13 par. 1 ed art. 14 par. 1 (sono più ampi del codice privacy)
- Sempre da indicare i contatti del DPO e base giuridica del trattamento, periodo di conservazione dei dati, logica dei processi di profilazione ecc.

TEMPI DELL'INFORMATIVA

- Nel caso di dati non raccolti direttamente presso l'interessato deve essere fornita entro un termine ragionevole MAI superiore ad 1 mese
- Oppure al momento della comunicazione dei dati a terzi o all'interessato



MODALITA' DELL'INFORMATIVA

- Concisa, trasparente, intellegibile e facilmente accessibile
- Linguaggio semplice e chiaro; uso combinato di ICONE
- Casi di esonero (artt. 13 par.4, 14 par. 5, 23 par.1)

C. Diritti degli interessati

- Copia dei dati – periodo di conservazione (o criteri) – garanzie in caso di trasferimento dei dati paesi 3i

- Anche dopo la revoca del consenso
- Obbligo di informare altri titolari che trattano stessi dati

- per i dati trattati in modo automatizzato
- Trattati su base consenso o contratto con interessato
- Dati forniti dall'interessato

- Esercitabile anche in caso di rettifica o opposizione al trattamento (dati vanno «contrassegnati»

C. Diritti degli interessati

Modalità esercizio diritti

1 mese è il termine di risposta all'interessato anche in caso di diniego

Spetta al titolare stabilire l'ammontare dell'eventuale contributo solo se si tratta di richieste eccessive o infondate o se richieste più copie dei dati personali

C. Diritti degli interessati

Modalità esercizio diritti

Risposta sempre per iscritto – oralmente solo se richiesto dall'interessato

Riscontro sempre in forma intellegibile concisa, trasparente e facilmente accessibile - con linguaggio semplice e chiaro

D. Titolare, responsabile, incaricato del trattamento

CONTITOLARITA’	Contratto disciplina i limiti di responsabilità	Interessato si può rivolgere ad entrambi per esercizio diritti
RESPONSABILE DEL TRATTAMENTO	contratto a contenuto minimo indicato (art. 28 par. 3)	Nomina sub-responsabili per specifiche attività (di cui risponde)
AUTORIZZATI AL TRATTAMENTO	«Vecchia» figura dell’incaricato non prevista nel regolamento	Non se ne esclude la presenza

E. Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili RESPONSABILIZZAZIONE DEL TITOLARE

Privacy by default

- Per impostazione predefinita trattare solo i dati personali nella misura strettamente necessaria alle finalità e per il tempo necessario: Si configura il trattamento prevedendo dall'inizio le garanzie per il rispetto dei requisiti del regolamento

Privacy by design

- Privacy dalla progettazione: Configurare il trattamento considerando il contesto (V.I.P.) ove avviene il trattamento stesso ed i rischi per i diritti e le libertà connesse

Valutazione Impatto Privacy

- Art. 35 Reg. Eu.
- Processo di valutazione interno
- N.B. vengono meno istituti di prior checking (verifica preliminare) e notifica preventiva trattamenti – l'intervento dell'Autorità Garante è sempre ex post

E. Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili
RESPONSABILIZZAZIONE DEL TITOLARE

Registro dei trattamenti

- Necessario per trattamenti a rischio libertà o titolari con > 250 dip.
- Forma scritta – anche elettronica
- Contiene le operazioni di trattamento con i contenuti dell'art. 30
- Deve essere esibito, su richiesta, al Garante

D.P.O. – R.P.D.

- Sensibilizzazione e formazione del personale
- Sorveglianza sullo svolgimento della valutazione di impatto
- Obbligatorio in alcuni casi (art. 37)

Misure di sicurezza

- Garantire un livello di sicurezza adeguato al rischio
- Art. 32: lista «aperta»
- Valutazione concreta rimessa al titolare a seguito della V.I.P.

Notificazione violazioni

- Data breach da notificare entro 72 ore e, comunque, senza ingiustificato ritardo.
- Solo se probabile rischio diritti e libertà interessati

F. Trasferimenti di dati verso paesi terzi e organismi internazionali

Solo se paese terzo «adeguato» (ossia rispetta requisiti stabiliti dalla Commissione ecc…)

Codici di condotta – schemi di certificazione per dimostrare garanzie adeguate – legittimano il trasferimento

Norme vincolanti d'impresa approvate dal Comitato europeo protezione dati – artt. 63-65

2) Come fare per mettersi in regola

Adempimenti	Art. GDPR	Azioni	Documenti da produrre
Mappa trattamenti	30	Compilare e tenere aggiornato registro trattamenti	Registro trattamenti

2) Come fare per mettersi in regola

Adempimenti	Art. GDPR	Azioni	Documenti da produrre
Sicurezza	32	• Compilare e tenere aggiornato il documento valutazione rischi • Esecuzione misure tecniche e organizzative inserite nel documento	Documento valutazione rischi
	35	• Verificare obbligo di compilazione • Chiedere parere DPO • Compilare e tenere aggiornato VIP • Esecuzione misure tecniche e organizzative inserite nel documento	Documento valutazione impatto privacy
	33-34	• Individuazione ufficio responsabile • Compilazione protocollo azioni • Verificare obbligo di compilazione • Chiedere parere DPO • Compilare e tenere aggiornato VIP • Esecuzione misure tecniche e organizzative inserite nel documento • Verifica sussistenza cause esonero • Compilare e tenere aggiornato registro violazione dati	Procedura data breach

2) Come fare per mettersi in regola

Adempimenti	Art. GDPR	Azioni	Documenti da produrre
Contitolari	26	• Stesura e sottoscrizione accordo contitolarità • Esecuzione misure tecniche e organizzative previste dall'accordo • Prevedere interfaccia unico nei confronti degli interessati	Accordo contitolarità
Nomine responsabili del trattamento	28	• Mappatura esternalizzazione dei trattamenti • Compilazione contratti con responsabili trattamento dati • Esecuzione misure tecniche e organizzative previste nel contratto • Mappatura sub-esternalizzazioni mediante inserimento apposita clausola nei contratti con responsabili se già esistenti oppure stesura e sottoscrizione nuovi contratti	Contratto del responsabile del trattamento
Nomine sub responsabili del trattamento			Contratto con sub responsabile

2) Come fare per mettersi in regola

Adempimenti	Art. GDPR	Azioni	Documenti da produrre
Nomine responsabili interni	5	• Mappatura nomine esistenti • Aggiornamento a nuovi compiti	Atto nomina e disciplinare
Nomine autorizzati	29	• Mappature nomine esistenti e allineamento con nuova normativa - aggiornamento a nuovi compiti	Nomine dipendenti e collaboratori
Formazione autorizzati	39	• Prevedere adeguata formazione per i soggetti autorizzati (corsi base – corsi soggetti apicali – corsi per DPO interni)	Corsi per soggetti autorizzati

2) Come fare per mettersi in regola

Adempimenti	Art. GDPR	Azioni	Documenti da produrre
Rapporti con interessati	12-13 -14	• Verifica informative esistenti e adeguamento alla nuova normativa (eventuale abbinamento a icone)	informativa
	6-7-8-9	• Verifica consensi esistenti e adeguamento alla nuova normativa • Cautele in caso di minori di età	Raccolta consenso, salvo esonero
RPD / DPO	37-38-39	• Verifica obbligo / opportunità di nomina • Scelta tra professionista / organizzazione esterna • Stesura e sottoscrizione nomina e contratto • Esecuzione misure previste nel contratto	Nomina RPD / DPO e contratto

2) Come fare per mettersi in regola

Adempimenti	Art. GDPR	Azioni	Documenti da produrre
Trasferimento dati estero - extra UE	44-50	• Verifica e rispetto condizioni di liceità (es. interesse legittimo – clausole contrattuali ecc.)	Condizioni di liceità
Certificazioni	42-43	• Acquisizioni certificazione • Esecuzione misure di mantenimento	certificazione
Codice di condotta	40-41	• Adesione a codice di condotta • Esecuzione misure di mantenimento	Codice di condotta

3) Sanzioni

Adempimento normativo	Sanzioni amministrative in caso mancato adempimento
Registro trattamenti	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Documento valutazione rischi	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Documento valutazione impatto privacy	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Procedura data breach	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Accordo contitolari	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Contratto con responsabili del trattamento	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Contratto con sub responsabili	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo

3) Sanzioni

Adempimento normativo	Sanzioni amministrative in caso mancato adempimento
Nomine dipendenti e collaboratori	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Corsi per gli autorizzati	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Informativa	Fino 10 mln/oppure se più elevato fino 4% fattura totale mondiale annuo
Raccolta consenso, salvo esonero	Fino 10 mln/oppure se più elevato fino 4% fattura totale mondiale annuo
Nomina DPO	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo
Trasferimento dati all'estero	Fino 10 mln/oppure se più elevato fino 4% fattura totale mondiale annuo
Certificazione	Fino 10 mln/oppure se più elevato fino 2% fattura totale mondiale annuo

GRAZIE PER L'ATTENZIONE

STUDIO LEGALE ASS.TO FACCIN SANTOLIN

Avv. Ivo Santolin – Avv. Anna Faccin

36070 Trissino (VI) Via Del Lavoro n. 45

36045 Lonigo (VI) Via E. Mazzadi n. 25

Tel e Fax 0445.490895

santolinivo@gmail.com

annafaccin@yahoo.it