15 febbraio 2018

-99 al GDPR 2016/679

La privacy per l'HR manager in vista dell'entrata in vigore del nuovo regolamento

LEXELLENT

Your partner in law.

LE NOVITÀ PIÙ SIGNIFICATIVE

Avv. Marco Giangrande

Condizioni per il consenso – Art. 7

- Richiesta di consenso: esplicita, distinguibile da altre questioni
- In forma comprensibile e facilmente accessibile
- Linguaggio semplice e chiaro
- Diritto di revoca in qualsiasi momento – (informato)
- Consenso dei minori è valido da 16 anni

Condizioni per il consenso

Il consenso è valido se ha tutte le caratteristiche indicate dal GDPR – Se no, raccogliere nuovo consenso!

Verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni dell'interessato

Formula comprensibile, semplice e chiara

Informativa – Artt. 13 e 14

Contenuti - *«garantire un trattamento corretto e trasparente»*

- Identità, dati contatto Titolare e Rappresentante
- Dati contatto DPO (Responsabile Protezione Dati)
- Finalità e base giuridica del trattamento
- Eventuali destinatari
- Eventuali trasferimenti a Paesi Terzi
- Periodo di conservazione o criteri utilizzati per determinazione

- Esistenza diritto accesso, rettifica, cancellazione, limitazione, opposizione al trattamento e portabilità
- Diritto di proporre reclamo autorità di controllo
- Se obbligo legale o contrattuale o requisito per la conclusione di un contratto e conseguenze mancata comunicazione
- Esistenza processo decisionale automatizzato e profilazione

Tempi dell'informativa

- Al momento in cui i dati personali sono ottenuti, in caso di raccolta presso l'interessato
- Entro un termine ragionevole che non può superare 1 mese, qualora i dati non siano ottenuti presso l'interessato

Modalità dell'informativa

- Forma: concisa, trasparente, intellegibile, accessibile
- Linguaggio: chiaro e semplice - (per minori*)
- Per iscritto e formato elettronico

- Cambio finalità -> Nuova informativa

… e quindi?

- Verificare la rispondenza delle informative attuali -> contenuti obbligatori e modalità di redazione
- Misure organizzative interne idonee per garantire il rispetto della tempistica

- Monitorare il cambio delle finalità -> Nuova informativa

I diritti degli interessati

1. Diritto di accesso – Art. 15
2. Diritto di cancellazione – Art. 17
3. Diritto di limitazione del trattamento – Art. 18
4. Diritto alla portabilità dei dati – Art. 20

Diritto di accesso – Art. 15

- Conferma che sia in corso un trattamento
- L'accesso ai dati personali
- Informazioni contenute nell'informativa
- Copia dei dati personali – che non deve ledere i diritti e le libertà altrui

Diritto di cancellazione – Art. 17

Diritto all'oblio, se i dati non più necessari, trattati illecitamente, cancellati per adempiere obbligo legale, revoca consenso

- Obbligo per Titolare di informare della richiesta altri titolari che trattano dati personali cancellati

Diritto di limitazione del trattamento – Art. 18

Esercitabile: violazione dei presupposti di liceità e per rettifica dei dati (in attesa di tale rettifica da parte del titolare)

-> Trattamenti vietati*, eccetto la conservazione

… e quindi?

Il dato personale deve essere **contrassegnato** -> misure idonee nei sistemi informativi

Diritto alla portabilità di dati – Art. 20

Per trattamenti automatizzati

Condizioni: - dati trattati consenso o contratto -> No interesse pubblico o legittimo del titolare - solo i dati «forniti» dall'interessato (C68)

… e quindi?

Linee guida del Gruppo Art. 29 – diritti terzi interessati, se dati ricompresi fra quelli relativi all'interessato.

Garante: bilanciamento diritti terzi e interessati

Misure -> formato interoperabile

I diritti degli interessati

Modalità per l'esercizio dei diritti – artt. 11 e 12

- Il Titolare agevola l'esercizio dei diritti ed è tenuto a dar riscontro - il Responsabile collabora
- Il T. adotta ogni misura tecnica e organizzativa idonea
- Termine per la risposta all'interessato: 1 mese
- In forma scritta
- Intellegibile, concisa, trasparente, accessibile – semplice e chiaro

I diritti degli interessati

Modalità per l'esercizio dei diritti – artt. 11 e 12

… e quindi?

Adottare misure tecniche e organizzative necessarie per favorire:

- Esercizio dei diritti
- Rispetto dei tempi
- Il riscontro alle richieste degli interessati

Titolare, responsabile, incaricato

- Titolare: determina finalità e mezzi del trattamento di dati personali
- Responsabile: tratta i dati personali per conto del T. – garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate …
- Incaricato: persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile

- Contitolari del trattamento – Art. 26 determinazione congiunta di finalità e mezzi di trattamento: Accordo Interno -> responsabilità e obblighi

Designazione Responsabile: contratto - Art. 28, p. 3

- Natura, durata e finalità del trattamento/i
- Categorie dati / interessati
- Misure tecniche e organizzative di sicurezza
- Obbligo di riservatezza per le persone autorizzate

Nomina di Sub-Responsabili – Art. 28, p. 4

Previa autorizzazione, scritta, specifica del Titolare

Il Responsabile primario risponde al Titolare dell'inadempimento del sub-responsabile

Obblighi specifici e distinti per Titolari e Responsabili:

- Registri dei trattamenti – Art. 30, p. 1 e 2
- Sicurezza dei trattamenti - Art. 32
- Nomina DPO – Art. 37

Titolari o Responsabili Extra-EU –> designazione Rappresentante in IT – Art. 27, p. 3 e Art. 3, n. 2*

… e quindi, cosa fare?

-> valutare esistenza di situazioni di contitolarità: obbligo accordo interno – Art. 26, p. 1

- Stabilire il «punto di contatto per gli interessati» -> esercizio dei diritti

-> verifica conformità nomina Responsabili – Art. 28, p. 3

-> integrazioni e modifiche Sub-Responsabili – «Autorizzati»

- Responsabile: adesione codici deontologici e schemi di certificazioni per dimostrare «garanzie sufficienti»

Data protection by default and by design - Art. 25

Protezione dei dati fin dalla progettazione e per impostazione predefinita

Approccio basato sul rischio specifico e prevedibile e su misure di responsabilizzazione di titolari e responsabili

Sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento

-> Analisi preventiva + impegno applicativo

Valutazione di impatto sulla protezione dei dati Art. 35 – 36

Valutazione di impatto: rischi, misure T&O e di sicurezza:

- Il Titolare inizia il trattamento o consulta Autorità
- *Ex-post*: misure correttive: ammonimento, limitazione o divieto

Registri delle operazioni di trattamento – Art. 30

Obbligo tenuta registro: tutti, eccetto <250 dipendenti, a meno che il trattamento sia rischioso

-> Supervisione Garante
-> Quadro aggiornato trattamenti
-> indispensabile per valutazione e analisi di rischio

… e quindi?

Accurata ricognizione trattamenti / caratteristiche

Misure di sicurezza - Art. 32

- Pseudonimizzazione e cifratura dati personali
- Assicurare riservatezza, integrità, disponibilità e resilienza sistemi e servizi di trattamento
- Ripristinare tempestivamente disponibilità/accesso in caso di incidente fisico o tecnico
- Procedure per testare, verificare e valutare periodicamente l'efficacia delle misure di sicurezza

Rischi: distruzione, perdita, modifica, divulgazione o accesso

Garante: linee guida e buone prassi

Notifica violazioni di dati personali – Art. 33 e 34

Titolari: notifica Autorità avvenuta violazione entro 72 ore, se probabile rischio per diritti e libertà interessati

- Non obbligatoria – valutazione del Titolare
- In caso di rischio elevato, obbligo di informare, senza ingiustificato ritardo, gli interessati

… e quindi?

-> documentare violazioni dati personali - circostante/conseguenze/provvedimenti

LEXELLENT

Your partner in law.

www.lexellent.it

Il materiale del corso è scaricabile alla pagina
http://lexellent.it/appuntamenti/gdpr-2016679/