IL NUOVO REGOLAMENTO GENERALE UE SULLA PROTEZIONE DEI DATI PERSONALI N. 679/2016: I NUOVI ADEMPIMENTI PRIVACY PER LE IMPRESE.

Presentazione

In data 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

Il Regolamento è entrato in vigore il 25 maggio 2016 senza necessità di recepimento con atti nazionali, ma sarà applicabile in tutti i Paesi UE solo a partire dal 25 maggio 2018. Il Regolamento sostituirà (salvi interventi normativi del Governo per alcune parti del Codice non sostituibili dal Regolamento, come gli aspetti sanzionatori penali) il "Codice Privacy" (D.Lgs. 196/2003, Codice in materia di protezione dei dati personali) in vigore dal 1 gennaio 2004.

Il Convegno, relatore il Prof. Avv. Alessandro del Ninno, è finalizzato ad offrire ai partecipanti una disamina pratica circa l'impatto in azienda della riforma europea della data protection, con la illustrazione di soluzioni organizzative ed operative volte alla conformità di processi e policies aziendali interne al quadro normativo privacy applicabile dal 2018.

Molte, infatti, le novità introdotte dal Regolamento: dagli obblighi di informativa rafforzati rispetto a quanto avviene ora con l'art. 13 del Codice Privacy alla novità - di grande impatto per le imprese – del "Registro dei trattamenti" (documento interno contenente informazioni essenziali in merito ai trattamenti svolti; dal principio c.d. dell'accountability preventiva di ogni trattamento(art. 35 del Regolamento, "Valutazione d'impatto sulla protezione dei dati") ai principi noti come "privacy by design" e "privacy by default" (art. 25 del Regolamento "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita") cioè la previsione di misure tecniche ed organizzative volte alla protezione dei dati personali già al momento della progettazione di un nuovo prodotto o software; dal nuovo diritto alla portabilità dei dati agli obblighi – ora generali – di notifica delle violazioni di dati personali ("data breach"). Nuova anche la figura del c.d. Data Protection Officer (DPO), ossia una figura prevista dall'art. 37 del Regolamento, interna o esterna all'azienda, e del tutto diversa dal responsabile del trattamento previsto dal Codice Privacy. Infine, importante l'aumento delle sanzioni amministrative, che potranno raggiungere la soglia di 20 milioni di euro o del 4% del fatturato mondiale totale annuo dell'esercizio precedente del trasgressore, se superiore: l'apparato sanzionatorio costituisce di certo un forte incentivo al rispetto della nuove prescrizioni.

PROGRAMMA

INTRIODUZIONE AL NUOVO REGOLAMENTO GENERALE UE SULLA PROTEZIONE DEI DATI PERSONALI.

Le principali novità introdotte dal Regolamento: cosa cambia e quali sono gli impatti e le ricadute pratiche sulle politiche del trattamento dei dati personali in azienda.

L'ambito di applicazione soggettiva e territoriale del Regolamento.

Entrata in vigore: il rapporto fra la attuale normativa e il Regolamento.

La tempistica di adeguamento delle politiche di trattamento dei dati alla nuova disciplina: la programmazione del cambiamento, la riorganizzazione delle procedure e la revisione delle istruzioni privacy.

LE NUOVE DEFINIZIONI GIURIDICHE DEI CONCETTI PRIVACY.

Il "dato personale": la nuova definizione.

Le categorie di dati personali: “dati di particolare natura”, “dati relativi alla salute”, “dati biometrici”, “dati genetici”. I dati ex sensibili e giudiziari nel nuovo Regolamento.

Le nuove definizioni: “limitazione del trattamento”, “pseudonimizzazione”, “profilazione”, “consenso dell’interessato”, “violazione di dati personali”, etc: le ricadute pratiche.

LE FIGURE SOGGETTIVE PRIVACY NEL REGOLAMENTO UE. ASPETTI ORGANIZZATIVI.

Il Titolare del trattamento: definizione, ruolo e poteri. Il caso dei “*joint controllers*”. Titolare del trattamento con più sedi nella UE e principio c.d dell’ *One Stop Shop*. Il Titolare del trattamento nell’ambito dei “gruppi imprenditoriali” come definiti dal Regolamento UE.

Il Responsabile interno del trattamento: definizione, nuova obbligatorietà della nomina e relative modalità, poteri e differenze di ruolo e funzione rispetto alla nuova figura del *Data protection Officer*.

Il Responsabile esterno del trattamento: le responsabilità dei fornitori di servizi esternalizzati e in *outsourcing*.

Le persone autorizzate al trattamento. Ruolo e poteri.

Altri soggetti coinvolti nel trattamento dei dati: il “rappresentante”, il “destinatario dei dati”, il “terzo”.

La nuova figura del *Data Protection Officer (DPO)*: quando è obbligatorio nominarlo. Caratteristiche soggettive e pre-requisiti della nomina. Ruolo e poteri del DPO all’interno dell’azienda. I rapporti gerarchici con gli altri soggetti privacy e le ricadute “lavoristiche” del DPO in azienda. Le Linee Guida sul DPO del Gruppo dei Garanti privacy UE del 13 Dicembre 2016.

I NUOVI ADEMPIMENTI ORGANIZZATIVI.

Il nuovo principio di accountability e la valutazione preventiva di impatto sulla protezione dei dati: caratteristiche e ipotesi di una corretta procedura aziendale di *Data Protection Impact Assessment.* Il principio di minimizzazione nel trattamento dei dati personali.

Privacy By Design e *Privacy By Default*: l’impatto dei nuovi princìpi obbligatori sui processi produttivi aziendali.

Il nuovo obbligo di Informativa: caratteristiche, contenuti, elementi informativi obbligatori e modalità di rilascio.

L’acquisizione del “consenso inequivocabile”. Modalità organizzative pratiche.

Il Registro Generale delle Attività di Trattamento e la mappatura dei flussi informativi: quando ne è obbligatoria la redazione e tenuta. Finalità, struttura e contenuti del Registro.

I nuovi obblighi di consultazione preventiva.

Le nuove misure di sicurezza nel trattamento dei dati personali: adempimenti pratici. I nuovi obblighi generali di notificazione della violazione di dati personali.

Le procedure a tutela dei diritti dell’interessato: il nuovo diritto all’oblio, cancellazione e la nuova portabilità dei dati. Il riscontro al diritto di accesso. La protezione dei minori. Class action.

Abolizione della Notificazione dei trattamenti all’Autorità garante per la protezione dei dati personali.

L'impresa certificata privacy: sigilli, codici di condotta e certificazioni. I percorsi di certificazione dei trattamenti.

IL MARKETING IN AZIENDA ALLA LUCE DEL NUOVO REGOLAMENTO UE. L'INTERNAZIONALIZZAZIONE DELL'IMPRESA E I NUOVI OBBLIGHI PER IL TRASFERIMENTO EXTRA UE DEI DATI PERSONALI

I trattamenti per finalità di marketing nel nuovo Regolamento: regole e procedure conformi.

La profilazione a scopi marketing: definizione e regole pratiche nel nuovo Regolamento UE.

Le regole sul trasferimento extra UE dei dati personali: casistica e adempimenti pratici aziendali da adottare. La prospettiva dei servizi cloud nel trasferimento all'estero dei dati personali. Trasferimento verso gli USA: il nuovo accordo *Privacy Shield.*

L'APPARATO SANZIONATORIO PREVISTO DAL REGOLAMENTO UE

Le nuove sanzioni e i controlli ispettivi. I poteri delle Autorità nazionali privacy.

Le nuove sanzioni amministrative pecuniarie.

Le sanzioni penali: permanenza delle sanzioni contenute nel Codice della privacy anche alla luce del Regolamento UE.

Sanzioni civilistiche e risarcimento del danno da trattamento dei dati personali: rapporto tra Codice della privacy e nuovo Regolamento UE.

Conclusioni.