EDDYSTONE

EDDYSTONE - LIGHTHOUSE

Il Regolamento UE sulla Privacy n. 2016/679 (GDPR)

Il Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali (il cosiddetto "GDPR"), già applicabile in via diretta in tutti i Paesi dell'Unione Europea e che sarà obbligatorio a partire dal 25 maggio 2018, richiede a tutte le imprese, studi professionali e pubbliche amministrazioni, l'adozione di misure organizzative e tecniche specifiche in materia di privacy.

Il GDPR abroga la precedente Direttiva Europea 95/46/CE, attuata in Italia con il D.Lgs n. 196 del 30 giugno 2003 ("Codice Privacy"), introducendo una vera e propria rivoluzione degli adempimenti privacy per tutte le imprese e gli istituti finanziari che offrono i propri servizi in Europa.

La protezione dei dati personali è un tema senz'altro rilevante per Banche, Intermediari finanziari, Assicurazioni, posta l'irrinunciabile esigenza di garantire la capacità di assicurare la riservatezza e la sicurezza dei dati e delle informazioni. Lo stesso Garante per la protezione dei dati personali italiano è intervenuto a dettare regole ad hoc per il trattamento dei dati personali nell'ambito di settori economici dei servizi finanziari e assicurativi. Tuttavia, il quadro attuale è destinato a cambiare sensibilmente nel breve periodo per effetto delle disposizioni del GDPR.

Il Garante italiano ha ritenuto opportuno offrire delle indicazioni al fine di facilitare l'applicazione delle nuove Disposizioni ed ha pubblicato la "Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali" e così supportare i soggetti pubblici e privati in questo delicato periodo di transizione alla nuova normativa privacy (per utilità si indica di seguito il relativo link: http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali).

L'aspetto più significativo, oltre il superamento della frammentazione normativa, è sicuramente il nuovo approccio della "responsabilizzazione" (account ability in inglese) di titolari e responsabili del trattamento– ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Il GDPR, infatti, non definisce requisiti specifici ma sposta la responsabilità, al titolare o responsabile del trattamento, di definire le misure di sicurezza idonee a garantire la corretta gestione dei dati personali trattati, dopo un'attenta analisi dei rischi. Dunque non ci saranno più misure minime, ma solo misure di sicurezza ed organizzative adeguate.

Workshop Eddystone Privacy GDPR - 1° marzo 2018

Il giorno **1° marzo 2018** si terrà il workshop gratuito organizzato da Eddystone, rivolto agli operatori del settore finanziario sui nuovi adempimenti previsti in materia di Privacy dal Regolamento GDPR.

Il workshop, organizzato insieme a Privacy Advisory Team (PAT), riguarderà anche tematiche operative quali le misure di sicurezza ed informatiche per la gestione delle informazioni conformi al GDPR. L'evento si terrà a Milano Via Delle Ore, 3 presso la sede dell'AMBROSIANEUM dalle ore 9:30 alle ore 13:00.

L'iscrizione può essere effettuata inviando una email all'indirizzo di posta direzione@eddystone.it

Registrati al Workshop

Eddystone Srl
Via della Moscova 40/7
20121 Milano
tel. 02 65 72 823
www.eddystone.it
Contatti:
Massimo Baldelli (AD)
Avv. Guido Pavan

SCHEDE & SCHEMI

Servizio in abbonamento:

- rassegna normativa
- approfondimenti
- checklist

Richiedi info a direzione@eddystone.it

ISCRIVITI ALLA NEWSLETTER

Countdown per i nuovi adempimenti previsti dal GDPR

Le imprese dovranno compiere una revisione completa dei dati che raccolgono e trattano, verificando le basi giuridiche per tali trattamenti e quale sia l'impatto di tali trattamenti per gli interessati.

Le imprese dovranno individuare e comprendere i principali cambiamenti che l'adeguamento alla nuova normativa privacy comporterà rispetto all'attuale disciplina. Questa valutazione, soprattutto per coloro che si avvalgono di servizi di full outsourcing informatici, non può prescindere dalle progettualità specifiche che anche i provider IT dovranno affrontare per i propri utenti.

Ecco, in sintesi, i principali impatti per l'organizzazione aziendale:

- LICEITA' DEL TRATTAMENTO: verifica dei dati trattati, con identificazione del tipo di dati e categorizzazione in modo da distinguerli tra loro, verifica della finalità e della sussistenza della base giuridica del trattamento;

- REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO: per le imprese o organizzazioni con più di 250 dipendenti- oppure sotto tale soglia, se il trattamento presenta (a) un rischio per i diritti e le libertà dell'interessato; (b) non è occasionale e include dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, relativi a condanne penali e a reati. Il Registro secondo le rispettive responsabilità e competenze - deve essere redatto sia dal titolare che dal responsabile del trattamento e rappresenta un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità e l'obbligo di rendicontazione;

- INFORMATIVA: adeguamento delle informative privacy, informando correttamente gli interessati della base giuridica del trattamento dei dati e dei loro diritti (rettifica, cancellazione, oblio) con l'indicazione del periodo per il quale i dati raccolti e trattati verranno conservati;

- DIRITTI DEGLI INTERESSATI: verifica della procedura per consentire agli interessati di richiedere l'attuazione dei loro diritti tra cui quello alla cancellazione e alla portabilità;

- ACCOUNTABILITY: adozione di misure tecniche e modelli organizzativi atti a garantire che la gestione e conservazione dei dati avvenga in maniera conforme ai principi di protezione dei dati personali. Attuazione dei principi di (1) "privacy by design", in base al quale i prodotti e i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti, cioè il trattamento deve essere previsto e configurato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati, e (2) "privacy by default" cioè di protezione dei dati per impostazione predefinita. Valutazione d'impatto del trattamento di talune tipologie di dati che presentino un rischio elevato inteso come valutazione dell'impatto negativo sulle libertà e i diritti degli interessati.

- DPO: eventuale designazione di un Data Protection Officer (DPO) che è un soggetto con competenze giuridiche, informatiche, di risk management, di analisi dei processi che ha il compito di valutare, organizzare e governare la gestione del trattamento dei dati nel rispetto della nuova normativa. Il DPO supporta il titolare e il responsabile del trattamento nell'adempimento al GDPR.

- DATA BREACH: instaurazione di una procedura per eventuali violazioni dei dati;

- TRAINING ADEGUATO: verifica della preparazione del personale ed eventuale aggiornamento, sulle nuove regole.

La figura del Data Protection Officer (DPO)

"Una figura che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati al fine di controllare il rispetto del GDPR, delle altre disposizioni in materia, nonché delle policy interne"

Il Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali (GDPR) introduce la figura del Responsabile della protezione dei dati (RPD), equivalente inglese di *Data Protection Officer* (DPO), ossia un soggetto avente una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati al fine di facilitare l'osservanza delle nuove disposizioni.

L'art. 37 GDPR prevede la designazione obbligatoria di un RPD per le autorità pubbliche e tutti i soggetti del settore privato le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala oppure nel trattamento su larga scala di categorie particolari di dati personali (dati sensibili).

La designazione obbligatoria di un RPD può essere prevista anche in casi ulteriori dalla legge nazionale o dal diritto europeo, ma, qualora non sia imposta specificatamente, è fatta salva, nonché consigliata, la facoltà di una nomina su base volontaria.

L'art. 39 GDPR individua i compiti del RPD, il quale, in particolare, si occupa di i) fornire consulenza in merito alla protezione dei dati, ii) vigilare sull'osservanza degli obblighi derivanti dal GDPR e da altre disposizioni in materia, nonché delle policy interne in materia di protezione dei dati personali, con particolare riferimento alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti, iii) fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati (DPIA), sorvegliandone lo svolgimento, e iv) cooperare con il Garante della Privacy fungendo inoltre da punto di contatto per questioni connesse al trattamento.

Il Responsabile della protezione dei dati può essere un dipendente del titolare o del responsabile del trattamento dei dati oppure assolvere i suoi compiti in base a un contratto di servizi purché, in ogni caso, adempia alle proprie funzioni in maniera indipendente e, qualora svolga altri compiti e funzioni, queste non diano adito ad un conflitto di interessi.

Non essendo prevista l'istituzione di un albo dei "Responsabili della protezione dei dati" che attesti la sussistenza dei requisiti di competenza e conoscenza spetta agli enti pubblici e alle società private procedere autonomamente alla selezione del Responsabile.

In merito, il quinto comma dell'art. 37 GDPR prevede che il RPD sia designato in funzione delle qualità professionali, prestando particolare attenzione alla conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e alla capacità di assolvere i propri compiti.

Nel processo di selezione e valutazione del RPD corre in aiuto lo stesso Garante della Privacy, il quale specifica che nella verifica delle competenze ed esperienze del RPD non sono richieste attestazioni formali o iscrizioni in appositi albi professionali, anche se la partecipazione a *master* o corsi di studio/professionali è da considerarsi un utile strumento nella valutazione del possesso di un adeguato livello di conoscenze.

In più, oltre alla conoscenza della normativa della privacy, è altrettanto importante la conoscenza delle norme e delle procedure amministrative caratterizzanti il settore di riferimento e il consiglio è quello di privilegiare quei soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito, documentando le esperienze concrete.

I prossimi eventi e convegni

Eddystone prosegue la collaborazione con i principali enti di formazione professionale rivolti agli intermediari finanziari attraverso la partecipazione in qualità di Relatore a convegni su temi specifici per il settore bancario-finanziario.

Tra i prossimi appuntamenti si segnala il seguente convegno:

"FinTech: nuovi approcci regolatori e servizi alla clientela" organizzato da Convenia che si terrà a Milano il prossimo **22 febbraio 2018** in cui Guido Pavan interverrà su "FinTech: una sfida di compliance"

Si ricorda che per l' **iscrizione a condizioni agevolate** al convegno Fintech del 22 febbraio 2017 in qualità di ospite Eddystone è possibile inviare un'email all'indirizzo direzione@eddystone.it specificando nel corpo dell'email il nominativo del partecipante.

Nell'ambito del percorso formativo sulla "Responsabilità amministrativa degli enti ex D.lgs. 231/2001" organizzato dall'Ordine dei Dottori Commercialisti e degli Esperti Contabili (ODCEC) di Milano e coordinato dal Guido Pavan, Segretario della Commissione Compliance e Modelli organizzativi si segnalano i seguenti convegni:

"Organismo di Vigilanza 231: costituzione, ruolo e responsabilità" che si terrà a Milano il **23 febbraio 2018** in cui Guido Pavan interverrà sul tema "Requisiti e composizione dell'OdV 231. Il ruolo, le funzioni e i poteri dell'OdV 231".

"L'attività dell'organismo di vigilanza 231: pianificazione e operatività" che si terrà a Milano il **9 marzo 2018** in cui Guido Pavan interverrà sul tema: "L'organizzazione dell'attività e l'adozione di un regolamento. Lo svolgimento delle verifiche e la tracciabilità delle attività" e Simona Sorgonà interverrà su "Le verifiche dell'ODV in materia antiriciclaggio".

Eddystone nel 2018 organizza i tradizionali workshop gratuiti sui seguenti temi:

- IV Direttiva Antiriciclaggio
- Controlli interni
- Whistleblowing
- MiFID 2

KEEP CALM AND CALL EDDYSTONE

Eddystone Srl
Via della Moscova 40/7
20121 Milano
Tel. +39 02.65.72.823
www.eddystone.it

Massimo Baldelli (AD)
m.baldelli@eddystone.it

Avv. Guido Pavan (partner)
g.pavan@eddystone.it

Seguici anche su

EDDYSTONE

WORKSHOP GRATUITO
Milano 1° marzo 2018

Il nuovo Regolamento sulla Privacy (GDPR)

Partecipazione libera per intermediari finanziari fino ad esaurimento posti (al massimo due partecipanti per intermediario). L'iscrizione può essere effettuata inviando una email all'indirizzo di posta direzione@eddystone.it

Registrati al workshop

INTERVENTI DEI RELATORI

Saluti e introduzione
Massimo Baldelli (AD, Eddystone)

Il regolamento GDPR e il suo recepimento in Italia. L'attività di assessment
Adriano Vinci (Avvocato, Eddystone, PAT Privacy Advisory Team)

La nuova figura del Data Protection Officer (DPO)
Guido Pavan e Arianna Locati (Eddystone)

Impatto della Cyber-Security sulla GDPR
Filippo Cavallarin (CEO, We are segment)

Coffee break

Impatti del GDPR sui sistemi informatici
Claudio Bettini e Sergio Mascetti (Università degli Studi di Milano, PAT Privacy Advisory Team)

L'anonimità come strumento per la protezione dei dati personali
Claudio Bettini e Sergio Mascetti (Università degli Studi di Milano, PAT Privacy Advisory Team)

Il regime sanzionatorio
Marco A. Morabito (Avvocato in Milano)

INFORMAZIONI E LOCATION

1° marzo 2018 dalle **9:30** alle **13:00**
AMBROSIANEUM Fondazione Culturale
Via Delle Ore, 3 Milano
Per info e iscrizioni: direzione@eddystone.it

WE ARE SEGMENT Detect & Protect

pat

MARCO MORABITO AVVOCATO

Ambrosianeum Fondazione Culturale