FenImprese
Federazione Nazionale Imprese - Industria - Sanità - Turismo

L.A.F.
LIBERA ASSOCIAZIONE FORENSE
Fasano - Cisternino
"Francesco Saponaro"

26 aprile 2018 – Laboratorio Urbano - Fasano

DALLA LEGGE SULLA PRIVACY AL GDPR

Nuova disciplina della Privacy alla luce del nuovo Regolamento UE 2016/679

COSA CAMBIA – COME ADEGUARSI

Graziano Albanese
ICT Consulting

FenImprese Brindisi Via Giovanni XXIII, 60 - Fasano (Br)
info@fenimpresebrindisi.it - Contact: 080.21.21.353

GDPR

Regolamento UE 2016/679

Parlamento Europeo 27 aprile 2016 applicabile dal 25 maggio 2018

Protezione delle **persone fisiche** con riguardo al trattamento dei dati personali e che abroga la direttiva 95/46/CE (Art. 4 ,1)

Viene recepito direttamente dagli stati membri una volta tradotto senza che venga appreso per essere attuato.

GDPR

Una battaglia da vincere sul campo.

Riferimenti normativi:

- D.LGS 85/2005 (Codice dell'amministrazione digitale)
- DPCM 1 Agosto 2015 (Misure minime di Sicurezza ICT per PA)
- Regolamento UE 2016/679 (GDPR)

Enti di riferimenti:

- Garante per la protezione dei dati
- Agenzia per l'Italia del Digitale

http://www.gazzettaufficiale.it/eli/id/2017/04/04/17A02399/sg

GDPR – Trattamenti leciti (Art. 6 – 7)

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte
c) il trattamento è necessario per adempiere un obbligo legale
d) il trattamento è necessario per la salvaguardia degli interessi vitali
e) il trattamento è necessario per l'esecuzione di un compito pubblico
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare

GDPR – Registro dei trattamenti (Art. 30)

Cosa contiene il registro dei trattamenti

a) nomi e contatti di: titolari e contitolari del trattamento, responsabili del trattamento e responsabile della protezione dei dati
b) le finalità del trattamento
c) descrizione delle categorie degli interessati e classificazione dei tipi di dati personali
d) categorie e destinatari oggetto di trasferimento dei dati trattati, sia nel territorio Paese ma anche a destinatari di paesi terzi o organizzazioni internazionali
e) le modalità e la documentazione delle garanzie per il trasferimento dei dati verso paesi terzi
f) i termini per la cancellazione delle categorie di dati
g) descrizione delle misure tecniche e organizzative

GDPR –Sicurezza del trattamento(Art. 33)

Data Breach Notification

- Obbligo della notifica da parte del titolare alle autorità, delle eventuali violazioni a meno che la violazione non presenti rischi per gli interessati.
- La notifica deve contenere la natura della violazione, il tipo di dati, i rischi, le conseguenze per gli interessati, le condizioni che hanno causato la violazione, le misure utilizzate per rimediare all'accaduto ed i contatti del responsabile della protezione dei dati per gli aggiornamenti e le informazioni aggiuntive.
- L'obbligo prevede la comunicazione da quando si è riscontrata la perdita di dati.

GDPR –Valutazione d'impatto sul trattamento dei dati (Art. 35)

- Prima di avviare un nuovo trattamento di dati ed in particolare in presenza di dati che presentano un rischio elevato per gli interessati, il titolare del trattamento avvia una valutazione di impatto su un trattamento o una serie di trattamenti.
- Il titolare si consulta con il responsabile della protezione dei dati se designato.
- Casi in cui si rende necessaria la valutazione di impatto: profilazione degli interessati, trattamenti su larga scala, dati relativi a condanne penali e a reati, sorveglianza sitemica di aree accessibili al pubblico.

GDPR – Data Protection Officer (Art.37 - 39)

Chi è? Quando bisogna nominarlo?
- Organismo pubblico (PA)
- In presenza di trattamenti che richiedono il monitoraggio regolare e sistemico su larga scala
- In presenza di categorie particolari di dati personali relativi a condanne e a reati (se su larga scala)
- In presenza di dati soggetti a profilazione

Compiti
- Informa e fornisce consulenza al titolare dei dati, sorveglia sull'osservanza del regolamento, fornisce supporto nella valutazione d'impatto, coopera con le autorità di controllo, funge da contatto fra le autorità ed il titolare.

GDPR – Informativa, diritti, portabilità

Art. 11 – 12 – 13 – 14 – 15 – 20

Cos'è e cosa deve contenere l'informativa

- Contatti di titolare, conitolare, responsabile e DPO
- Periodo di conservazione dei dati
- Diritti degli interessati

Diritti degli interessati
- Accesso ai dati personali (quali dati e come sono stati ottenuti e come vengono elaborati)
- Portabilità dei dati (trasferimento o possibilità di portare via i propri dati)

GDPR – Sanzioni

Art. 83

- Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.
- Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso
- Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.
- In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente

GDPR –Sicurezza del trattamento(Art. 32)

Misure tecniche organizzative adeguade.

- Pseudonimizzazione
-Riservatezza, integrità e resilienza dei dispositivi e dei sistemi di trattamento
- Capacità di ripristino dei dati e loro accesso dapo un incidente etecnico o fisico (disaster recovery)
- Procedure di auditing periodiche delle misure tecniche e organizzative

Obiettivi e misure adeguate di sicurezza:

- Dispositivi (inventario dei dispositivi autorizzati)
- Software (inventario dei software autorizzati)
- Protezione delle configurazioni hardware e software (immagini e backup)
-Le vulnerabilità (valutazione e correzione continua)
- I privilegi di accesso a dispositivi e software
- Difese contro i malware
- Copie di sicurezza
-Protezione dei dati

Strumenti per affrontare e adeguarsi alle misure minime di sicurezza:

- Misure tecniche
- Misure organizzative

Strumenti per le adeguate misure di sicurezza:

Misure tecniche

Firewall

- Sistemi per il monitoraggio dei dispositivi e dei software
- Difesa contro i malware
- Protezione dati
- Log e IPS

Server e sistemi da backup

- Protezione dei dati (crittografia)
- Protezione dei livelli di accesso
- Log degli accessi

Strumenti per le adeguate misure di sicurezza:
Misure organizzative

- Serie di regole che ben definiscono le modalità operative per il trattamento dei dati durante le fasi di lavoro e la loro conservazione in archivio cartaceo ed elettronico
- Scelta e definizione dei profili di accesso ai tipi di dati (chi può accedere e a cosa)
- Tutte le regole e le procedure necessarie per un adeguato trattamento.

FenImprese

Federazione Nazionale Imprese - Industria - Sanità - Turismo

L.A.F.
LIBERA ASSOCIAZIONE FORENSE
Fasano - Cisternino
"Francesco Saponaro"

GRAZIE PER L'ATTENZIONE

Graziano Albanese
ICT Consulting

FenImprese Brindisi Via Giovanni XXIII, 60 - Fasano (Br)
info@fenimpresebrindisi.it - Contact: 080.21.21.353