Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci & C. Srl
(cda)

Associazione Protezione diritti e libertà privacy APS
(Vice presidente)

Contatti:
dileo@studiopaciecsrl.it
Cell. 3931019939
www.consulenzepaci.it
Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICQ SICEV)

Consulente per l'implementazione dello schema di certificazione ISDP@10003
(Ente di certificazione INVEO)

Lead Auditor ISO 27001 , aggiornamento ISO 27701

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
PERCHE' ?

(1) La tutela dei dati personali è sempre più un'esigenza di tutti, il legislatore europeo ha predisposto negli ultimi anni una serie di nuove direttive europee, e di regolamenti proprio per tutelare i diritti e le libertà delle persone nell'ambito dei servizi dell'informazione, che ad oggi sono gestiti da «pochi» big player sul mercato mondiale, e che impattano non solo sulla nostra vita quotidiana ma anche nell'ambito lavorativo.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

(2) L'utilizzo di nuove tecnologie e la loro evoluzione continua comporta una costante revisione delle misure di garanzia per i fruitori di questi servizi.

(3) Con l'evoluzione tecnologica si evolvono anche le minacce sulla sicurezza informatica ed i relativi incidenti, violazioni di dati personali, che comportano non solo danni economici, reputazionali, ma anche perdita di riservatezza e danni fisici che impattano sulla salute delle persone.

(4) I fruitori dei servizi non sono solo i consumatori ma anche le organizzazioni che utilizzano queste nuove tecnologie per il loro business.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

(5) Ancora ad oggi l'errore umano costituisce una delle maggiori vulnerabilità nella sicurezza informatica;

(6) La prima misura di garanzia che ciascuna persona fisica può adottare è la conoscenza;

(7) la consapevolezza si costruisce con la formazione e il suo continuo aggiornamento.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

Nel Regolamento UE 2016/679 le «istruzioni» devono essere intese come formazione, a riguardo il Regolamento:

(8) include nelle misure di sicurezza la formazione, che quindi diventa obbligatoria (art. 32)
(9) ogni soggetto che effettua trattamenti dati per conto del Titolare del trattamento o del Responsabile deve essere istruito (art. 29)
(10) Le istruzioni devono essere specifiche per i trattamenti dati affidati agli incaricati (art. 2 quaterdecies D.Lgs 196/2003)
(11) Le misure di sicurezza, fra cui la formazione, devono essere adeguate «allo stato dell'arte», ovvero al corrente progresso tecnologico (art. 32 e art. 5) - vedi punto (2)
(12) Le misure di sicurezza devono essere aggiornate e revisionate qualora necessario (art. 24), ENISA: almeno una volta all'anno, e almeno una volta ogni 6 mesi per rischio elevato
(13) Il titolare del trattamento deve dimostrare che il trattamento dati è conforme al Regolamento (art. 24)

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

Nel Regolamento UE 2016/679 le «istruzioni» devono essere intese come formazione, a riguardo il Regolamento:

(8) nelle misure di sicurezza è inclusa la formazione, che quindi diventa obbligatoria (art. 32)

Piano di formazione aziendale che preveda:
le modalità di erogazione, la tipologia dei corsi, la calendarizzazione nel tempo

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

Nel Regolamento UE 2016/679 le «istruzioni» devono essere intese come formazione, a riguardo il Regolamento:

(9) ogni soggetto che effettua trattamenti dati per conto del Titolare del trattamento o del Responsabile deve essere istruito (art. 29)

Elenco degli incaricati al trattamento dati con l'indicazione della formazione svolta
Attestati di formazione o altre evidenze documentate

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

Nel Regolamento UE 2016/679 le «istruzioni» devono essere intese come formazione, a riguardo il Regolamento:

(10) Le istruzioni devono essere specifiche per i trattamenti dati affidati agli incaricati (art. 2 quaterdecies D.Lgs 196/2003)

Il piano di formazione deve prevedere contenuti specifici per i trattamenti dati svolti delle organizzazioni a prescindere che siano titolari o responsabili per detti trattamenti dati.
Esempi:
«gestione personale dipendente» per chi tratta i dati dei dipendenti,
«amministratori di sistema» per chi svolge tale ruolo o semplicemente può impostare o stabilire nuovi utenti con specifici diritti di accesso per software o servizi

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
MA PERCHE' ?

Nel Regolamento UE 2016/679 le «istruzioni» devono essere intese come formazione, a riguardo il Regolamento:

(11) Le misure di sicurezza, fra cui la formazione, devono essere adeguate «allo stato dell'arte», ovvero al corrente progresso tecnologico – vedi punto (2)

AGGIORNAMENTO ANNUALE
COSA C'E' DI NUOVO

Servizi dell'informazione:

DSA – Digital Service Act (Reg. UE 2022/2065)

nuovo regolamento europeo che prevede una serie di regole e obblighi per le piattaforme online al fine di garantire una maggiore responsabilità e trasparenza nel trattamento dei contenuti online e nella protezione dei diritti dei consumatori. In particolare, il DSA stabilisce nuove regole per la rimozione dei contenuti illegali o dannosi, promuove la concorrenza equa e prevede maggiori obblighi di trasparenza e responsabilità per le piattaforme digitali.

DMA – Digital Market Act (Reg. UE 2022/1925)

nuovo regolamento europeo sui mercati digitali, ha la finalità di regolare l'operatività delle grandi società tecnologiche e contrastare gli abusi di posizione dominante delle piattaforme online che agiscono come "gatekeeper" (controllori dell'accesso) in relazione ad un insieme di servizi che rappresentano per le imprese importanti punti di accesso per raggiungere gli utenti finali.

Settore finanziario:

DORA – Resilienza Operativa digitale per il settore finanziario (Dir. UE 2022/2554)

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

AI – Intelligenza Artificiale (Regolamento n. 1689 del 13 giugno 2024)

un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

Dove impatta (qualche esempio):

Sanità:

I sistemi di intelligenza artificiale nell'ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa alla professione medica.

Lavoro:

L'intelligenza artificiale è impiegata per migliorare le condizioni di lavoro, tutelare l'integrità psico-fisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone in conformità al diritto dell'Unione europea…. Il datore di lavoro o il committente è tenuto a informare il lavoratore dell'utilizzo dell'intelligenza artificiale …

Autorità Giudiziaria:

È sempre riservata al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento.

Modifiche al codice penale:

Chiunque, al fine di arrecare nocumento a una persona e senza il suo consenso, ne invia, consegna, cede, pubblica o comunque diffonde l'immagine, un video o la voce, falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da sei mesi a tre anni. Se dal fatto deriva un danno ingiusto, la pena è della reclusione da uno a cinque anni.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Sicurezza informatica:

NIS2 e decreto cybersecurity (Dir. UE 2022/2555 che abroga la precedente NIS1 a partire dal 17 ottobre 2024)
Si applica a soggetti pubblici e privati sulla base dei servizi resi, delle caratteristiche economiche e di mercato.

Settori a cui si applica a prescindere dalla dimensione economica dell'organizzazione:

- fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;
- prestatore di servizi di fiducia;
- registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
- Soggetti che presentano un influenza importante per determinati servizi svolti;
- Pubbliche amministrazioni centrali, o regionali che potrebbero avere un determinato impatto sulla sicurezza;

Medie imprese (n. dipendenti da 50 a 250 o da 10 a 50 mil. euro fatturato) che rientrano nei settori:

Settori critici (Allegato 1)
Energia e affini, trasporto, banche, infrastrutture dei servizi finanziari, sanità, acque, infrastrutture digitali, fornitori di servizi di telecomunicazione B2B, pubblica amministrazione (non tutte), spazio.

Altri settori critici (Allegato 2)
Servizi postale, sostanze chimiche, gestione dei rifiuti, alimenti, fabbricazione (elenco), fornitori di servizi digitali.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Sicurezza informatica:

NIS2 e decreto cybersecurity (Dir. UE 2022/2555 che abroga la precedente NIS1 a partire dal 17 ottobre 2024)

Attività da porre in essere: (devono essere declinate per ciascuna organizzzione)

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
b) gestione degli incidenti;
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;
g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Sicurezza informatica:

NIS2 e decreto cybersecurity (Dir. UE 2022/2555 che abroga la precedente NIS1 a partire dal 17 ottobre 2024)

Attività da porre in essere: (devono essere declinate per ciascuna organizzazione)

Riepilogo delle macro attività:

- Registrazione sul portale nazionale (se l'azienda rientra nel perimetro)
- Organizzazione dei processi per raggiungere la conformità
- Creare il Team NIS 2
- Revisione ed aggiornamento della gestione degli asset aziendali per confermare il profilo di rischio
- Raccogliere gli audit e le risultanze delle verifiche effettuate anche sulla base delle altre normative di riferimento al fine di inserirli nel processo NIS 2
- Eliminare le complessità dell'infrastruttura - Semplificazione

Cos'è un incidente di sicurezza per la NIS 2:

tutti gli eventi che compromettono la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi. Un incidente è significativo se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato o se si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Sicurezza informatica:

Linee guida ACN – Agenzia per la Cybersicurezza Nazionale (tenuta delle password, crittografia, etc.)
https://www.acn.gov.it/portale/home

Conservazione delle Password:
La maggiorparte delle organizzazioni e tutti i gestori di servizi di informatica rientrano nelle nuove linee guida della ACN, introdotte con un provvedimento del Garante per la Protezione dei Dati Personali.
Maggiore sicurezza !

ENISA – Agenzia Europea per la Sicurezza Informatica
linee guida che saranno integrate di volta in volta nelle procedure e nelle istruzioni

https://www.enisa.europa.eu/

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Strumenti di lavoro:

Meta-dati della posta elettronica e log «traccianti»

PROCEDURA DI SEMPLIFICAZIONE DELLO STUDIO PACI PER PICCOLE ORGANIZZAZIONI

Provvedimento 6 giugno 2024 *«Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati»*
Riferimenti normativi: Art. 88 GDPR - art. 4, comma 1, l. 20/5/1970, n. 300, espressamente richiamata dall'art. 114 del Codice.

Definizione Garante Metadati: *«informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client (le postazioni terminali che effettuano l'invio dei messaggi e che consentono la consultazione della corrispondenza in entrata accedendo ai mailbox elettroniche, definite negli standard tecnici quali MUA – Mail User Agent)»*
«operazioni di invio e ricezione e smistamento dei messaggi possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, in relazione al sistema di gestione del servizio di posta elettronica utilizzato, anche l'oggetto del messaggio spedito o ricevuto.»

Fino a 21 gg. la conservazione può essere necessaria per il corretto funzionamento della posta elettronica.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Strumenti di lavoro:

Whistleblowing - D.Lgs 24/2023
e relativi aggiornamenti sulla base delle risultanze a seguito della nostra partecipazione al tavolo di lavoro ANAC

Corrette basi giuridiche, consensi ove necessario, portale per le segnalazioni e non l'email, indagine sull'applicazione da parte dell'ANAC

Marketing e tempi di conservazione dei consensi e dei relativi dati personali.
Provvedimenti del Garante, trasparenza delle informazioni di primo e secondo livello, semplificazione.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Sanità:

Fascicolo Sanitario elettronico 2.0 – FAQ Garante
Il FSE è stato previsto dall'art. 12, del d.l. n. 179/2012 e successivamente disciplinato dal Dpcm n. 178/2015 e dal decreto del 7 settembre 2023 (FSE 2.0).
- Oscuramento rafforzato rispetto agli atti amministrativi.

DSE - Dossier Sanitario Elettronico
Ancora ad oggi questo sconosciuto…

Ricerca scientifica – Modifica della normativa di riferimento nel D.Lgs. 196/2003 - FAQ Garante
Semplificazione - consenso non obbligatorio per diverse casistiche

Oblio Oncologico – Schede e FAQ Garante
L'oblio oncologico è definito dalla legge 7 dicembre 2023, n. 193, come il diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica, nei limiti indicati dalla predetta legge, per l'accesso ai servizi bancari, finanziari, di investimento e assicurativi, in sede di indagini sulla salute dei richiedenti un'adozione e per l'accesso alle procedure concorsuali e selettive, al lavoro e alla formazione professionale.

AGGIORNAMENTO ANNUALE DELLA FORMAZIONE
COSA C'E' DI NUOVO

Videosorveglianza dei comuni e dei soggetti privati:

- Sicurezza urbana integrata, fototrappole, collegamento con Forze dell'ordine, Sistemi di lettura targhe, etc.

- Accordi sindacali più specifici, indicazioni DTL, cartelli, informative, tempi di conservazione, etc…

Aspetti sul controllo del lavoratore derivante dai trattamenti dati relativi alla registrazione dei

«file log»
«backup metadati posta elettronica»
«log navigazione internet»

a seguito di alcuni provvedimenti sanzionatori del Garante per la Protezione dei dati

Chiederemo di integrare alcune informazioni rispetto ai sistemi informatici

Penetration test sulla sicurezza dell'infrastruttura informatica

Abbiamo registrato diversi incidenti e databreach
occorsi sia a società private che a pubbliche amministrazioni,

è giunta l'ora di effettuare penetration test sulla sicurezza dell'infrastruttura informatica

al fine di scongiurare hackeraggi, eventi malevoli, phishing,

ma anche al fine di essere compliance al regolamento per la privacy by default,

e le misure di sicurezza di cui all'art. 32 che prevedono la verifica costante dell'efficacia delle misure di sicurezza implementate.

PER QUESTO A SEGUIRE UNA SESSIONE FORMATIVA DI AGGIORNAMENTO SULLE MISURE DI SICUREZZA E SULLA CIBERSICUREZZA, CHE OGNUNO DI NOI PUO' METTERE IN ATTO PER NON COMPROMETTERE LA SICUREZZA DELL'INFRASTRUTTURA INFORMATICA AZIENDALE.