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 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Il biennio 2024-2025 rappresenta un periodo di significativa evoluzione normativa nell'ambito della protezione dei dati personali, con l'introduzione di nuovi regolamenti europei e il recepimento di direttive che ampliano e rafforzano il quadro giuridico esistente.

Queste novità non solo si affiancano e integrano il Regolamento Generale sulla Protezione dei Dati (GDPR), ma affrontano anche le nuove sfide poste dall'innovazione tecnologica, dall'intelligenza artificiale e dalla crescente digitalizzazione.

Analizziamo di seguito le principali normative entrate in vigore a metà e fine 2024 e per il 2025, delineando gli impatti sui diritti degli interessati e sugli obblighi per le organizzazioni.

Non dimentichiamo la costante necessità di elevare le misure di sicurezza / cybersecurity, come non mai oggi gli attacchi informatici e il phishing sono oltremodo pericolosi!!!

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

- ✓ **Linee guida 2/2023 sull'ambito tecnico dell'art. 5(3) della direttiva ePrivacy - Versione 2.0 – adottato il 7 ottobre 2024**
- ✓ **AI – Intelligenza Artificiale (Regolamento n. 1689 del 13 giugno 2024)**
- ✓ **Data Act: applicabile dal 12 Settembre 2025 - Regolamento (UE) 2023/2854,**
- ✓ **eIDAS 2: Nuove Regole per l'Identità Digitale - Regolamento (UE) 2024/1183, noto come eIDAS 2, è entrato in vigore il 20 maggio 2024.**
- ✓ **Videosorveglianza PA, comuni e soggetti privati (provvedimenti del Garante)**
- ✓ **La Privacy in Condominio – nuove linee guida del 8 maggio 2025 per la gestione degli adempimenti da parte degli amministratori di condominio e per il condominio stesso, compresa la videosorveglianza.**
- ✓ **NIS2 – Rafforzamento delle misure organizzative per la sicurezza. Soggetti Importanti e Soggetti Essenziali.**
- ✓ **TELEMEDICINA**

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Data Act: applicabile dal 12 Settembre 2025 - Regolamento (UE) 2023/2854

è entrato in vigore l'11 gennaio 2024, ma sarà pienamente applicabile solo dal 12 settembre 2025.

Il Data Act stabilisce norme armonizzate sull'accesso equo ai dati e sul loro utilizzo, definendo in particolare i diritti di accesso ai dati generati dall'uso di prodotti connessi o servizi correlati. Questo regolamento mira a:

- Facilitare il passaggio tra fornitori di servizi di trattamento dati
- Migliorare l'interoperabilità dei dati e dei meccanismi di condivisione
- Imporre ai fabbricanti e ai fornitori di servizi l'obbligo di consentire agli utenti l'accesso ai dati generati dall'uso dei loro prodotti o servizi

Il Data Act influenzerà profondamente sia il mercato business-to-business che business-to-consumer, costringendo tutti i fornitori di servizi di trattamento dati ad apportare modifiche alle loro condizioni contrattuali e ai loro processi operativi entro settembre 2025.

Attuazione:
- 11 gennaio 2024: Entrata in vigore del Data Act.
- 12 settembre 2025: Applicazione diretta del regolamento in tutti gli Stati membri dell'UE.
- 12 gennaio 2027: Entrata in vigore delle disposizioni relative alla rimozione delle spese di commutazione tra fornitori di servizi di trattamento dei dati

Continua…

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Data Act: applicabile dal 12 Settembre 2025 - Regolamento (UE) 2023/2854

Come ricade indirettamente agli sviluppatori di servizi / siti web ?

1) Progettare la raccolta dati in modo trasparente e conforme e garantire che i dati generati dall'uso del sito o servizio (es. dati degli utenti, log, tracciamenti) siano accessibili agli utenti finali e al titolare del sito.

2) Implementare meccanismi chiari per l'esportazione e la portabilità dei dati (es. scaricamento dei dati utente in formato standardizzato).

3) Facilitare la condivisione dei dati con terze parti, ovvero l'architettura software deve consentire all'utente di condividere i propri dati con soggetti esterni (ad es. per ottenere assistenza, analisi, servizi personalizzati).

4) Predisporre API o strumenti che permettano il trasferimento sicuro e controllato dei dati verso soggetti terzi, se richiesto.

5) Evitare clausole contrattuali sbilanciate/abusive: nei contratti con i clienti, non imporre limitazioni eccessive sull'uso dei dati da parte del cliente (es. vietare l'esportazione, imporre esclusiva sull'hosting).

6) Consentire all'utente la piena titolarità e controllo dei propri dati (consentire decisioni sui dati generati attraverso il sito o servizio)

7) Garantire portabilità e interoperabilità: usare formati aperti e standardizzati (es. JSON, CSV, XML) per l'archiviazione dei dati e per l'eventuale estrazione.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Data Act: applicabile dal 12 Settembre 2025 - Regolamento (UE) 2023/2854

Come ricade indirettamente ad uno sviluppatore di servizi web ?

8) Facilitare la migrazione dei dati in caso di cambio fornitore del servizio web o di hosting, ed evitare tecnologie proprietarie che rendano difficile il passaggio ad altri fornitori.

9) Prevedere una corretta gestione del consenso «privacy» dove necessario sia nei banner che nei form: integrare banner cookie conformi al GDPR e alla direttiva ePrivacy (con scelte libere e chiare, "Rifiuta tutto" e "Accetta tutto", eliminare finalità con frasi generiche del tipo «migliorare l'esperienza», attenzione all'utilizzo della base giuridica del «legittimo interesse» – non legittima!).

10) Progettare i servizi secondo i principi di privacy by design e privacy by default (pensare ai corretti adempimenti privacy prima di mettere in linea un sito web)

11) Consentire agli utenti di accedere, correggere, cancellare o esportare i propri dati (diritti dell'interessato, art. 15–22 GDPR).

12) Supportare la compliance del cliente: fornire documentazione tecnica e strumenti per aiutare i clienti a rispettare gli obblighi del Data Act e della normativa sulla privacy. (manuali, istruzioni, configurazioni corrette degli utenti non generici, etc…)

13) Implementare misure di sicurezza (senza aspettare che lo chieda il cliente): adottare misure tecniche e organizzative adeguate per proteggere i dati (es. cifratura, doppia autenticazione, logging – file log).

14) Documentare tutti i processi per la gestione degli incidenti, anche se non comportano violazioni di dati personali ed in caso di incidente comunicarlo senza ritardo al cliente, sarà lui a valutare se è un data-breach o meno in qualità di responsabile.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Linee guida 2/2023 sull'ambito tecnico dell'art. 5(3) della direttiva ePrivacy
Versione 2.0 – adottato il 7 ottobre 2024

Dove impattano le linee guida – estensione del campo di applicazione dell'art. 5 par. 3 della direttiva ePrivacy:

«…l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato…»

1. Fingerprinting dei dispositivi

Il fingerprinting è quella tecnologia che raccoglie caratteristiche uniche del dispositivo dell'utente (es. sistema operativo, risoluzione dello schermo, font installati, fuso orario, tipo di browser). Se utilizzata per creare un profilo identificativo univoco, anche senza cookie, necessita di consenso, salvo finalità strettamente tecniche.

2. Pixel di tracciamento (utilizzato per tracciare attività utenti, es. apertura email)

Un piccolo elemento invisibile (1x1 pixel) inserito in email o pagine web che, al caricamento, invia informazioni al server (es. IP, orario, tipo di dispositivo, click, posizione del mouse, etc.).

3. Elaborazione locale con trasmissione dei dati

Anche se l'elaborazione inizia localmente, il fatto di raccogliere ed esportare dati dal terminale richiede il rispetto della ePrivacy, quindi serve consenso, salvo eccezioni.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Linee guida 2/2023 sull'ambito tecnico dell'art. 5(3) della direttiva ePrivacy
Versione 2.0 – adottato il 7 ottobre 2024

Dove impattano – estensione del campo di applicazione dell'art. 5 par. 3 della direttiva ePrivacy:

4. Tracciamento basato solo su indirizzi IP

Identificare e tracciare gli utenti attraverso il loro indirizzo IP pubblico, anche senza altri identificatori. L'IP (considerato dal GDPR dato personale) può essere usato per riconoscere il dispositivo nel tempo. Se ciò avviene senza scopo tecnico essenziale, rientra nell'art. 5(3) e richiede il consenso.

5. Segnalazione intermittente e mediata da dispositivi IoT

Dispositivi intelligenti (es. frigoriferi, contatori smart, assistenti vocali) che trasmettono dati periodici tramite protocolli o sensori anche passivamente. Ogni accesso o raccolta dati da questi dispositivi è considerato un «accesso all'apparecchiatura terminale». Se non è necessario per la funzione richiesta, richiede il consenso.

6. Forte integrazione della direttiva ePrivacy con il GDPR, anche nei termini di Autorità sanzionatoria.

Tutte queste tecnologie vanno valutate non solo per il tipo di dati, ma per il fatto che accedono o registrano informazioni nel dispositivo dell'utente, che è l'aspetto centrale della direttiva ePrivacy.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

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

Principi fondamentali da rispettare:

1) Protezione dei dati fin dalla progettazione – Applicazione della proc. Privacy by Design ed Accountability

Analizzare gli adempimenti rispettivamente al trattamento dati e incorporare misure di tutela dei dati personali sin dalle prime fasi di utilizzo, implementazione o sviluppo di applicazioni o sistemi di IA, come previsto dall'articolo 25 del GDPR. (es. ChatGPT, Copilot, Perplexity, Gemini, etc…)

Es. quali sono i soggetti interessati per il trattamento dei dati ? Dipendenti, clienti, utenti, fornitori…

2) Trasparenza e supervisione umana:

Informare sull'utilizzo della AI anche per i sistemi a «basso rischio» (es. chatbot, centralini, generazione testi, etc.) - informativa art. 13 GDPR sull'utilizzo di sistemi di AI Garantire che le decisioni automatizzate siano comprensibili e che vi sia sempre la possibilità di intervento umano.

3) Non discriminazione algoritmica:

Evitare che gli algoritmi perpetuino o amplifichino discriminazioni esistenti (es. analisi di un CV), assicurando equità nei processi decisionali. Suggerimento / obbligo di effettuare una **F.R.I.A.** (Foundamental Rights Impact Assesment) per i sistemi a medio / elevato rischio

4) Limitazione della raccolta dei dati:

Raccogliere solo i dati strettamente necessari per le finalità specifiche del trattamento, evitando l'uso eccessivo o non autorizzato delle informazioni personali. (es. posso creare un preventivo anche senza nomi del clienti…)

5) Accortezze ed attenzioni – Politiche aziendali per l'utilizzo della AI – Istruzioni – Approvazione dell'organizzazione !!!

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

eIDAS 2: Nuove Regole per l'Identità Digitale - Regolamento (UE) 2024/1183

Il regolamento eIDAS 2.0 (Regolamento UE 2024/1183), entrato in vigore il 20 maggio 2024, rappresenta un'evoluzione significativa del quadro normativo europeo per l'identità digitale e i servizi fiduciari. Questo aggiornamento mira a creare un ecosistema digitale più sicuro, interoperabile e user-centric, con impatti rilevanti per cittadini, imprese e pubbliche amministrazioni.

Principali novità di eIDAS 2.0 – (fra cui: Firme elettroniche, digitali, PEC, sigilli, marche temporali, certificati di autenticità, registri elettronici, conservazione qualificata, firma remota senza dispositivi, etc.)

1. European Digital Identity Wallet (EUDI Wallet)
introduzione dell'EUDI Wallet, un portafoglio digitale che consente ai cittadini europei di:

- Conservare e gestire le proprie credenziali digitali (es. carta d'identità, patente, certificati).
- Autenticarsi online e firmare documenti digitalmente.
- Controllare quali dati condividere e con chi, migliorando la privacy e la sicurezza.

L'EUDI Wallet sarà riconosciuto in tutti gli Stati membri, facilitando l'accesso a servizi pubblici e privati a livello transfrontaliero.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

eIDAS 2: Nuove Regole per l'Identità Digitale - Regolamento (UE) 2024/1183

Principali novità di eIDAS 2.0

2. Nuovi servizi fiduciari qualificati

eIDAS 2.0 amplia l'elenco dei servizi fiduciari, includendo:

- Attestazione elettronica degli attributi: certificazioni digitali di caratteristiche specifiche di una persona o entità (es. titoli di studio, licenze).
- Gestione di dispositivi qualificati per la creazione di firme elettroniche a distanza: servizi che permettono la firma digitale senza la necessità di dispositivi fisici.
- Registri elettronici: sistemi per la registrazione sicura e verificabile di dati elettronici.
- Archiviazione elettronica qualificata (eArchiving): servizi per la conservazione a lungo termine di dati e documenti elettronici, garantendone integrità e leggibilità.

Obiettivi: standardizzare e rafforzare la fiducia nelle transazioni digitali in tutta l'UE.

3. Interoperabilità e standardizzazione

eIDAS 2.0 promuove l'adozione di standard tecnici comuni e l'interoperabilità tra i sistemi di identità digitale dei diversi Stati membri, riducendo le barriere tecniche e legali per l'accesso ai servizi digitali transfrontalieri.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

eIDAS 2: Nuove Regole per l'Identità Digitale - Regolamento (UE) 2024/1183

Principali novità di eIDAS 2.0

per le imprese e gli sviluppatori

Le organizzazioni che sviluppano software e servizi web dovranno:

- Adeguare i sistemi di autenticazione: integrare l'EUDI Wallet come metodo di identificazione e autenticazione.
- Supportare i nuovi servizi fiduciari: adattare le piattaforme per utilizzare i servizi di attestazione, firma elettronica a distanza, registri elettronici e archiviazione qualificata.
- Garantire la conformità normativa: assicurarsi che le soluzioni offerte rispettino i requisiti di sicurezza, privacy e interoperabilità stabiliti da eIDAS 2.0.
- Formare il personale: aggiornare le competenze del team per gestire le nuove tecnologie e normative introdotte.

Attuazione:
- 20 maggio 2024: Entrata in vigore del regolamento eIDAS 2.0.
- Entro il 21 maggio 2025: Pubblicazione degli atti esecutivi (Implementing Acts) che definiranno le specifiche tecniche e operative per l'attuazione del regolamento.
- Entro il 24 dicembre 2026: Gli Stati membri dovranno rendere disponibile l'EUDI Wallet ai cittadini.
- Entro il 24 dicembre 2027: Le imprese obbligate dovranno accettare l'identificazione tramite EUDI Wallet.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

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 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

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 249 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 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

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 organizzaione)

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 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

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 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

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 – **UNA DELLE MAGGIORI CRITICITA' ALGORITMI OBSOLETI – ES. «MD5»**

La maggior parte 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 informatica !

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

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

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Strumenti di lavoro:

Meta-dati della posta elettronica e log «traccianti»

IMPLEMENTAZIONE DELLA PROCEDURA DI SEMPLIFICAZIONE DELLO STUDIO PACI PER PICCOLE ORGANIZZAZIONI CHE NON RICHIEDE L'AUTORIZZAZIONE DELLA DTL

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 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Marketing e tempi di conservazione dei consensi e dei relativi dati personali.

Provvedimenti del Garante, trasparenza delle informazioni di primo e secondo livello, semplificazione.

Concetti generali da ricordare:

- **Informative su due livelli** (informativa breve e informativa completa)

- **Il consenso per il marke**ting (es. invio newsletter) se raccolto opportunamente **NON SCADE!**

Tuttavia ricordare all'utente che ha prestato un consenso dopo X anni dando la possibilità di recedere rafforza il principio di accountability e previene eventuali sanzioni. E' sempre suggerita una DPIA nei casi di un alto volume di contatti.

- **Anche il consenso della profilazione NON SCADE!**

La durata della conservazione dei dati profilati però deve essere limitata ad una finestra temporale di 1 anno, se superiore obbligo di DPIA - Valutazione di Impatto per il titolare del trattamento.

- **Non confondiamo le basi giuridiche:** il contratto non è un consenso, il legittimo interesse solo per i clienti già acquisiti e solo per comunicazioni via email

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

Videosorveglianza PA, comuni e soggetti privati

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

Un importante provvedimento sanzionatorio inflitto al Comune di Levanto sulla videosorveglianza pone in evidenza come ancora ad oggi non siano adottate e recepite le prescrizione del GDPR nell'ambito della videosorveglianza.

1) In particolare per la predisposizione della Valutazione di Impatto – DPIA – prima di iniziare il trattamento dati, prima di mettere in funzione un impianto di videosorveglianza.

2) I comuni non possono utilizzare i sistemi di lettura targhe per la sicurezza urbana a meno che non sono previsti nei Patti per la Sicurezza sottoscritti con la Prefettura.

3) I contenuti dei cartelli per la videosorveglianza devono contenere, oltre alle informazioni standardizzate anche i trattamenti dati che più impattano sulle persone (es.

4) La necessità di avere credenziali utente «ad personam» riferibili ad un singolo dipendente / persona, e non generalizzate o di gruppo.

AGGIORNAMENTO ANNUALE 2025
COSA C'E' DI NUOVO E COSA CI «PORTIAMO DIETRO» DAL 2024

TELEMEDICINA e normativa correlata

Impatto della Telemedicina su Organizzazioni Sanitarie alla Luce del GDPR e del Decreto 196/2003:

L'implementazione della telemedicina in Italia (2024-2025) richiede un adeguamento normativo rigoroso, con particolare attenzione al GDPR (Regolamento UE 2016/679) e al Decreto Legislativo 196/2003 (Codice Privacy).

Farmacie	Informativa, Consenso esplicito, crittografia dati, nomina incaricati, etc.
Strutture sanitarie private, ambulatori, case di riposo	DPIA, pseudonimizzazione, tracciabilità accessi, etc.
Laboratori analisi	DPIA, Integrazione FSE con consenso, crittografia referti
Medici	Adesione informata specifica, informativa, uso piattaforme certificate
Fornitori tecnologici	Verifica dei ruoli, Accordi Art. 28 GDPR, conformità dispositivi

Chiederemo di integrare alcune informazioni rispetto a:

1) sistemi informatici e alla Cybersecurity!

2) aspetti sul controllo del lavoratore derivante dai trattamenti dati relativi alla registrazione dei «file log», «metadati e back-up posta elettronica»

3) Utilizzo di applicazione di AI Intelligenza Artificiale

Penetration test sulla sicurezza dell’infrastruttura informatica

Abbiamo registrato molti 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.

NON RINUNCIATE AL CORSO SULLA CYBERSECURITY PER TUTTI I DIPENDENTI CHE UTILIZZANO DISPOSITIVI ELETTRONICI ED INFORMATICI