Laboratorio del Cittadino APS
Associazione di Promozione Sociale

PRIVACY E SICUREZZA ONLINE

INDIS
Inclusione Digitale Senior

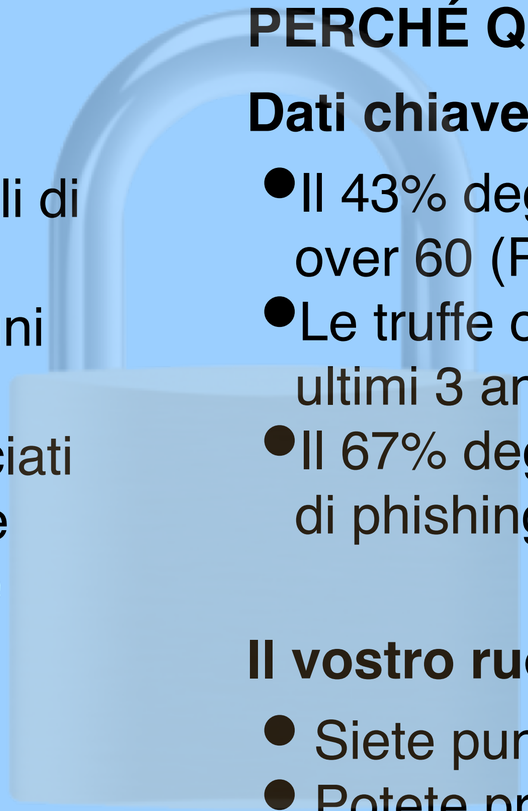
Corso per responsabili di associazioni di adulti e senior
PROGETTO INDIS: INCLUSIONE DIGITALE SENIOR

Privacy e Sicurezza Informatica Guida pratica per responsabili di associazioni

Obiettivi del corso:

- Comprendere i concetti fondamentali di privacy e sicurezza digitale
- Riconoscere i rischi online più comuni
- Acquisire strumenti pratici per proteggere sé stessi e i propri associati
- Sviluppare competenze per educare adulti e senior alla sicurezza digitale

Durata: 2-3 ore



PERCHÉ QUESTO CORSO È IMPORTANTE

Dati chiave:

- Il 43% degli attacchi informatici colpisce utenti over 60 (Rapporto Clusit 2023)
- Le truffe online sono aumentate del 135% negli ultimi 3 anni
- Il 67% degli anziani non sa riconoscere una email di phishing

Il vostro ruolo è cruciale:

- Siete punto di riferimento per la vostra comunità
- Potete prevenire truffe e violazioni della privacy
- Aiutate a costruire una cultura digitale sicura

INTRODUZIONE - IL MONDO DIGITALE OGGI

La trasformazione digitale:

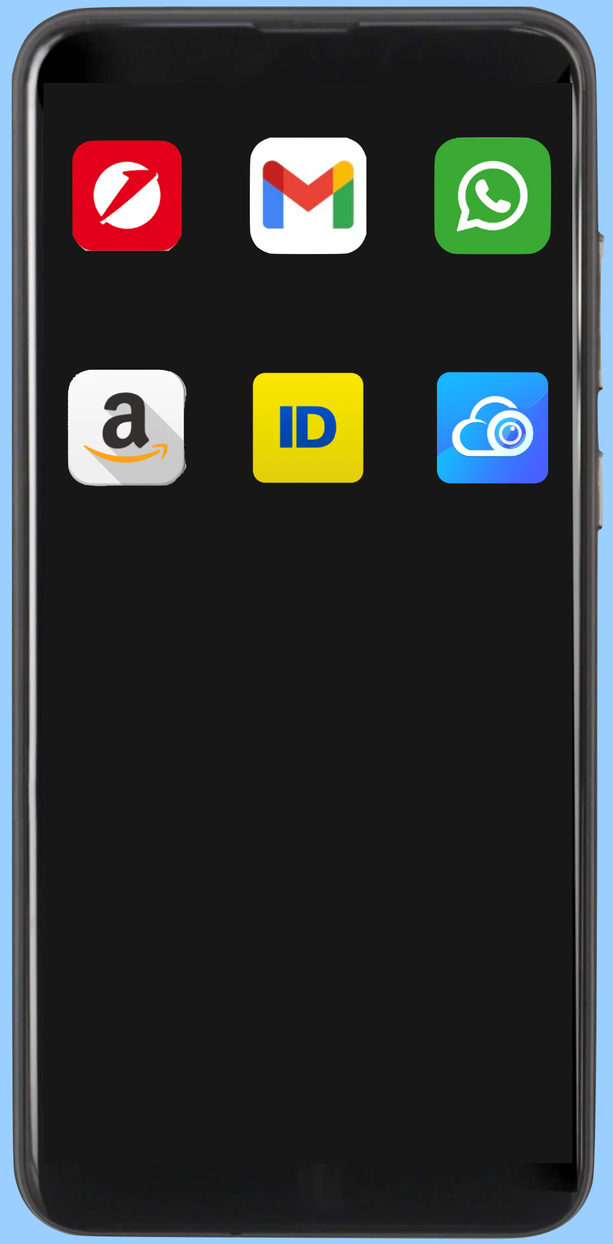
- Servizi bancari online
- Comunicazione via email e messaggistica
- Social media e videochiamate
- Acquisti online e e-commerce
- Servizi pubblici digitali (SPID, CIE, Fascicolo Sanitario)

Opportunità e rischi:

✅ Maggiore connessione e autonomia

❌ Esposizione a minacce informatiche

❌ Vulnerabilità per chi ha meno competenze digitali



COS'È LA PRIVACY DIGITALE

Definizione: La privacy digitale è il diritto di controllare quali informazioni personali vengono raccolte, come vengono utilizzate e con chi vengono condivise nel mondo digitale.

Tipi di dati personali:

- **Dati identificativi:** nome, cognome, codice fiscale, indirizzo
- **Dati sensibili:** salute, opinioni politiche, religione
- **Dati biometrici:** impronte digitali, riconoscimento facciale
- **Dati comportamentali:** cronologia di navigazione, acquisti, posizione GPS

Principio fondamentale: I tuoi dati appartengono a te!

LA PRIVACY COME DIRITTO FONDAMENTALE

1. Fondamento Costituzionale e Normativo

In Italia:

- **Art. 15 della Costituzione:** tutela della libertà e segretezza della corrispondenza e di ogni forma di comunicazione
- **Codice della Privacy** (D.Lgs. 196/2003 e successive modifiche)

A livello europeo:

- **Art. 8 della Carta dei diritti fondamentali dell'UE:** protezione dei dati personali
- **GDPR** (Regolamento UE 2016/679): standard più avanzato al mondo per la protezione dei dati

A livello internazionale:

- **Art. 12 della Dichiarazione Universale dei Diritti Umani:** protezione contro interferenze arbitrarie nella vita privata

2. Protezione della Dignità Umana

La privacy digitale tutela:

- **L'intimità personale:** pensieri, emozioni, relazioni private
- **L'autonomia decisionale:** libertà di scelta senza condizionamenti
- **L'identità personale:** chi siamo senza essere costantemente osservati o giudicati

3. Libertà di Espressione e Pensiero

Senza privacy:

- Le persone si autocensurano
- Si riduce il dibattito libero e aperto
- Si limitano ricerca, creatività e innovazione
- Si teme il giudizio costante (effetto "panopticon digitale")

4. Protezione da Discriminazioni

I dati personali possono essere usati per:

- Discriminazioni lavorative (salute, orientamento politico)
- Esclusione da servizi (assicurazioni, credito)
- Manipolazione e profilazione
- Controllo sociale e sorveglianza di massa

5. Sicurezza Personale ed Economica

La violazione della privacy può portare a:

- **Furto di identità:** uso fraudolento di dati personali
- **Frodi finanziarie:** accesso a conti bancari e carte di credito
- **Ricatti e estorsioni:** basati su informazioni sensibili
- **Stalking e molestie:** attraverso dati di localizzazione e contattI

CONSEGUENZE DELLA VIOLAZIONE DELLA PRIVACY

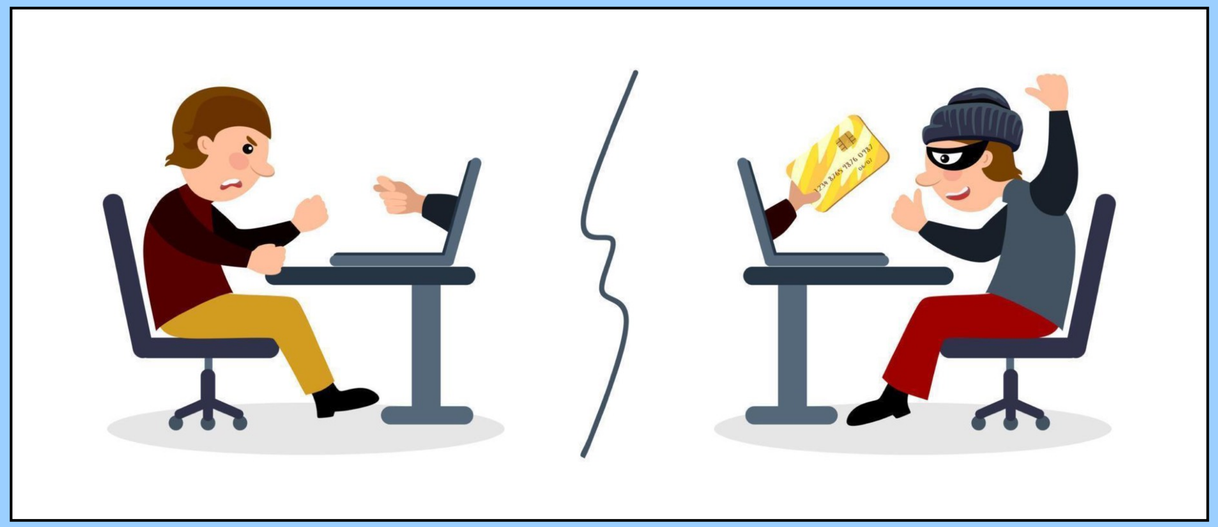
Rischi concreti:

📧 Spam e marketing aggressivo

- Telefonate indesiderate
- Email pubblicitarie invasive

💰 Frodi finanziarie

- Furto di identità
- Accesso non autorizzato ai conti bancari



🎯 Manipolazione

- Pubblicità mirata basata su dati personali
- Truffe personalizzate

😔 Impatto emotivo

- Stress e ansia
- Perdita di fiducia nella tecnologia
- Isolamento sociale

PRIVACY ONLINE - PERCHÉ È CRUCIALE

Il mondo online è permanente:

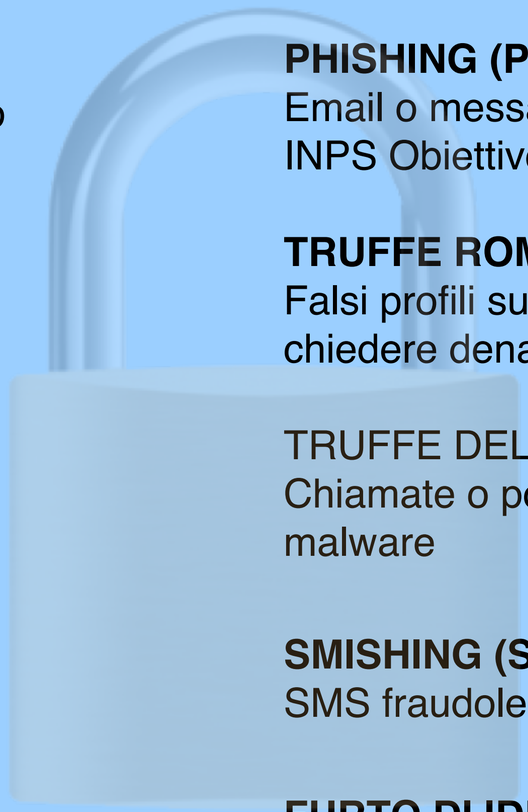
- Ciò che pubblichi online rimane per sempre
- I dati possono essere copiati e condivisi all'infinito
- La cancellazione completa è quasi impossibile

Chi raccoglie i tuoi dati:

- Social media (Facebook, Instagram, WhatsApp)
- Motori di ricerca (Google, Bing)
- Siti web e app
- Servizi cloud
- Dispositivi smart (smartphone, smart TV)

Cosa fanno con i tuoi dati:

- Profilazione per pubblicità mirata
- Vendita a terze parti
- Analisi comportamentali
- Addestramento di intelligenze artificiali



I PRINCIPALI RISCHI ONLINE PER ADULTI E SENIOR

PHISHING (Pesca di dati)
Email o messaggi falsi che sembrano provenire da banche, poste, INPS Obiettivo: rubare credenziali e dati personali

TRUFFE ROMANTICHE
Falsi profili su social o siti di incontri che instaurano relazioni per chiedere denaro

TRUFFE DEL FALSO SUPPORTO TECNICO
Chiamate o popup che dichiarano problemi al computer per installare malware

SMISHING (SMS phishing)
SMS fraudolenti su pacchi in consegna, bollette, vincite

FURTO DI IDENTITÀ
Uso improprio di dati personali per aprire conti, contratti, commettere reati

SICUREZZA ONLINE

ESERCIZIO 1 - RICONOSCERE IL PHISHING

Analizzate questi esempi e identificate i segnali di allarme:

Esempio A: "Gentile cliente, il suo conto Poste Italiane è stato bloccato per motivi di sicurezza. Clicchi qui entro 24 ore per riattivarlo: http://poste-sicurezza.tk/login"

Esempio B: "Buongiorno, sono Marco della sua banca. Abbiamo notato un'attività sospetta. Mi può confermare il codice che le arriverà via SMS?"

Segnali di allarme: 🚩 Senso di urgenza 🚩 Link sospetti (controllare il dominio) 🚩 Errori grammaticali 🚩 Richiesta di dati sensibili 🚩 Mittente non verificabile 🚩 Minacce o promesse irrealistiche

STRATEGIA 1 - PASSWORD SICURE

Caratteristiche di una password forte:

- Almeno 12 caratteri
- Combinazione di maiuscole, minuscole, numeri, simboli
- Nessuna parola del dizionario
- Nessun dato personale (date di nascita, nomi)

❌ **Password deboli:**

- 123456
- password
- nomecognome
- datanascita

✅ **Password forte esempio:**

- M!laNo2024$Sole (frase trasformata)
- r7$Kp9@mL2vX (casuale)

Regole d'oro:

1. Una password diversa per ogni servizio importante
2. Cambiare password se si sospetta una violazione
3. Mai condividere le password
4. Usare un gestore di password (LastPass, 1Password, Bitwarden)

STRATEGIA 2 - AUTENTICAZIONE A DUE FATTORI (2FA)

Cos'è: Un secondo livello di sicurezza oltre alla password

Come funziona:

1. Inserisci username e password
2. Ricevi un codice temporaneo via SMS, app o email
3. Inserisci il codice per accedere

Vantaggi:

- Anche se qualcuno scopre la tua password, non può accedere senza il secondo fattore
- Ricevi notifiche di tentativi di accesso sospetti

Dove attivarla:

- Account email (Gmail, Outlook)
- Home banking
- Social media
- SPID e servizi pubblici

Consiglio pratico: Attivare sempre la 2FA per servizi bancari e email principale!

STRATEGIA 3 - NAVIGAZIONE SICURA

Verificare i siti web: 🔒 **Controllare il lucchetto** nella barra degli indirizzi (HTTPS)

🔍 **Leggere attentamente l'URL** (attenzione a caratteri strani o domini sospetti) ✅ **Usare siti ufficiali** per servizi importanti

Browser sicuri e aggiornati:

- Chrome, Firefox, Safari, Edge (sempre aggiornati)
- Attivare la protezione contro siti pericolosi
- Cancellare periodicamente cronologia e cookie

Reti Wi-Fi: ❌ Evitare operazioni sensibili su Wi-Fi pubblici (bar, stazioni) ✅ Usare connessione dati o VPN per operazioni bancarie 🏠 Proteggere il Wi-Fi di casa con password forte

Download sicuri:

- Scaricare solo da fonti ufficiali
- Verificare estensioni file (.exe, .zip possono contenere virus)
- Mai aprire allegati sospetti

STRATEGIA 4 - SOFTWARE DI SICUREZZA

Antivirus e Anti-malware:

Opzioni gratuite affidabili:

- Windows Defender (integrato in Windows 10/11)
- Avast Free
- AVG Free

Opzioni a pagamento:

- Norton
- Kaspersky
- Bitdefender

Funzioni essenziali: ✓ Scansione in tempo reale ✓ Protezione da ransomware ✓ Firewall ✓ Protezione email e web

Aggiornamenti software:

- Sistema operativo (Windows Update)
- Browser
- Applicazioni
- Antivirus

Regola: Installare sempre gli aggiornamenti di sicurezza!

STRATEGIA 5 - GESTIONE DEI SOCIAL MEDIA

Impostazioni privacy su Facebook:

1. Chi può vedere i tuoi post → Solo amici
2. Chi può cercarti → Limita la visibilità pubblica
3. Richieste di amicizia → Controlla chi può inviarti richieste
4. Revisione tag → Attiva l'approvazione prima della pubblicazione

Buone pratiche: ❌ Non condividere: indirizzo di casa, numero di telefono, posizione in tempo reale ❌ Non accettare amicizie da sconosciuti ❌ Non cliccare su link sospetti nei messaggi ✅ Verificare le impostazioni privacy ogni 6 mesi ✅ Pensare prima di pubblicare: "Vorrei che questa informazione fosse pubblica per sempre?"

WhatsApp:

- Impostare privacy "Solo contatti" per foto profilo, info e ultimo accesso
- Disattivare conferme di lettura se desiderato
- Verificare l'identità cambiando il codice di sicurezza

STRATEGIA 6 - EMAIL E MESSAGGISTICA SICURA

Gestione email:

Prima di cliccare su un link:

1. Passa il mouse sopra senza cliccare (vedi URL reale)
2. Verifica il mittente (indirizzo email completo)
3. Chiediti: "Mi aspettavo questa email?"

Segnali di email fraudolenta:

- Mittente sconosciuto o strano
- Richieste urgenti
- Errori di ortografia
- Allegati inaspettati
- Link abbreviati o sospetti

Protezione: ✅ Non rispondere a email sospette ✅ Segnalare come spam ✅ Contattare direttamente l'ente attraverso canali ufficiali ✅ Mai fornire password via email

Messaggistica:

- Verificare identità di chi chiede denaro o informazioni
- Usare app crittografate (WhatsApp, Signal, Telegram)

ESERCIZIO 2 - CASO PRATICO

Scenario: Maria, 68 anni, socia della vostra associazione, riceve una telefonata:

"Buongiorno signora, sono dell'assistenza Microsoft. Il suo computer ha un virus pericoloso. Dobbiamo intervenire immediatamente. Mi permette di accedere da remoto al suo PC? Le invio un link…"

Domande per il gruppo:

1. Quali sono i segnali di allarme in questa situazione?
2. Cosa dovrebbe fare Maria?
3. Come responsabili, come la consiglieresti?

Discussione guidata (5-10 minuti)

BRAINSTORMING RISPOSTE:

COSA FARE IN CASO DI VIOLAZIONE

Se sospetti un problema:

Cambia immediatamente le password

- Account compromesso
- Altri account con stessa password

Controlla gli accessi

- Verifica attività recenti
- Disconnetti tutti

STRUMENTI PRATICI PER LA SICUREZZA

Checklist di sicurezza digitale:

Settimanale: □ Controllare estratti conto bancari □ Verificare attività sospette sugli account

Mensile: □ Aggiornare software e sistema operativo □ Cambiare password di servizi critici (ogni 3-6 mesi) □ Fare backup dei dati importanti

Semestrale: □ Rivedere impostazioni privacy social media □ Eliminare account non utilizzati □ Controllare quali app hanno accesso ai dati

Risorse utili:

- **Have I Been Pwned** (haveibeenpwned.com) - verifica se la tua email è stata violata
- **VirusTotal** (virustotal.com) - scansiona file sospetti
- **Password Strength Checker** - testa la forza delle password

RISCHI ASSOCIATI ALL'USO DI DISPOSITIVI IoT E SMART DEVICES

I dispositivi IoT (Internet of Things) sono oggetti fisici dotati di sensori, software e connettività che raccolgono ed elaborano dati, comunicando tramite Internet senza intervento umano, per automatizzare processi e migliorare efficienza, esempi includono smartwatch, termostati intelligenti, telecamere di sicurezza, macchinari industriali, e persino componenti di città intelligenti, offrendo comodità e nuovi servizi, ma richiedendo anche attenzione alla sicurezza

VULNERABILITÀ DI SICUREZZA

Password Deboli o Predefinite

- Molti dispositivi IoT vengono venduti con password di default (es. "admin/admin")
- Gli utenti raramente cambiano queste credenziali
- Gli hacker possono facilmente accedere usando database di password predefinite
-

RISCHI SPECIFICI PER ADULTI E ANZIANI

Complessità di Configurazione

- Interfacce complicate
- Impostazioni di sicurezza nascoste
- Difficoltà nel gestire aggiornamenti
- Mancanza di supporto tecnico accessibile

Truffe Mirate

- Finte chiamate di supporto tecnico
- Accesso remoto richiesto per "riparazioni"
- Installazione di malware mascherato da aggiornamenti

Falso Senso di Sicurezza

- Fiducia eccessiva nella tecnologia
- Credere che "smart" significhi "sicuro"
- Non comprendere i rischi reali
-

COME EDUCARE I VOSTRI ASSOCIATI Strategie didattiche efficaci:

1. **Linguaggio semplice e concreto**
   - Evitare tecnicismi
   - Usare esempi della vita quotidiana
   - Fare paragoni con il mondo fisico

2. **Approccio pratico**
   - Dimostrazioni dal vivo
   - Esercitazioni guidate
   - Supporto individuale

3. **Creare un ambiente sicuro**
   - "Non esistono domande stupide"
   - Valorizzare l'esperienza
   - Imparare dagli errori

4. **Materiali di supporto**
   - Guide stampate con caratteri grandi
   - Video tutorial semplici
   - Linea di supporto per dubbi

5. **Ripetizione e follow-up**
   - Ripassare concetti chiave
   - Incontri periodici
   - Gruppo di mutuo aiuto

PARTECIPARE ALLE NOSTRE ATTIVITÀ FORMATIVE ALL'INTERNO DEL PROGETTO INDIS: INCLUSIONE DIGITALE SENIOR

STATISTICHE RECENTI SU VIOLAZIONI DELLA PRIVACY E DATA BREACH

Dati Globali ed Europei (2024-2025)

Sanzioni GDPR

- **1,2 miliardi di euro** di sanzioni totali in Europa nel 2024 (calo del 33% rispetto al 2023)
- **5,88 miliardi di euro** totali di sanzioni dal 2018 (entrata in vigore del GDPR)
- Le sanzioni dimostrano l'attenzione crescente delle autorità sulla protezione dei dati

Violazioni dei Dati

- **Oltre 1 milione di alert** per dati compromessi sul dark web nel primo semestre 2025
- **33.700 casi** di dati esposti sul web aperto (in aumento)
- **86,7%** dei dati compromessi proviene dal dark web
-

Dati Italia (2024-2025)

Sanzioni GDPR in Italia

- **237,3 milioni di euro** di sanzioni nel 2024
- **5° posto in Europa** per ammontare delle sanzioni
- Crescente attenzione alla governance dei dati personali

Attacchi Informatici

Secondo il **Rapporto Clusit 2025**:

- **357 attacchi gravi** contro organizzazioni italiane nel 2024 (39% del totale 2020-2024)
- **+53% di attacchi informatici** nel primo semestre 2025 rispetto allo stesso periodo 2024
- **1.549 attacchi** registrati nel primo semestre 2025
- **10,2% degli attacchi globali** colpisce l'Italia (1 su 10)
- L'Italia è uno dei paesi più colpiti al mondo

Dati Compromessi

Secondo **CRIF (2025)**:

- **6° posto mondiale** per indirizzi email compromessi
- **36,4% degli utenti italiani** ha ricevuto almeno un alert per dati compromessi
- **Regioni più colpite:** Lazio, Lombardia, Sicilia, Campania

Record di Data Breach

- Numero record di violazioni di dati nel 2024-2025
- Aumento significativo di siti web compromessi o messi offline
-

FONTI

1. **DLA Piper** - GDPR Fines and Data Breach Survey (Gennaio 2025)
2. **Rapporto Clusit 2025** - Associazione Italiana per la Sicurezza Informatica
3. **CRIF** - Report dati compromessi primo semestre 2025
4. **ICT Business** - Report sanzioni GDPR Italia/Europa (Febbraio 2025)

ADESSO ENTRIAMO NELLO SPECIFICO DELLA PRIVACY, DI COSA SI TRATTA, COSA COMPORTA PER AZIENDE E ASSOCIAZIONI, ADEMPIMENTI LEGALI E BUONE PRATICHE

BUONE PRATICHE PER LA CONSERVAZIONE DI DATI SENSIBILI

Guida per Aziende e Associazioni in conformità con l'ordinamento italiano

QUADRO NORMATIVO ITALIANO ED EUROPEO

Normative di Riferimento

1. **GDPR (Regolamento UE 2016/679)**
   - Normativa principale europea sulla protezione dati
   - Direttamente applicabile in Italia dal 25 maggio 2018
   - Sanzioni fino a 20 milioni di euro o 4% del fatturato globale

2. **Codice Privacy Italiano (D.Lgs. 196/2003)**
   - Modificato dal D.Lgs. 101/2018 per adeguamento al GDPR
   - Integra e specifica il GDPR per il contesto italiano

3. **Linee Guida del Garante Privacy**
   - Provvedimenti e linee guida specifiche
   - Interpretazioni e chiarimenti per settori specifici

4. **Normative Settoriali**
   - Sanità: Fascicolo Sanitario Elettronico
   - Lavoro: Statuto dei Lavoratori (L. 300/1970)
   - Sicurezza: NIS2 (Direttiva cybersecurity)

PRINCIPI FONDAMENTALI DEL GDPR

1. Liceità, Correttezza e Trasparenza
I dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

2. Limitazione della Finalità
Raccolti per finalità determinate, esplicite e legittime.

3. Minimizzazione dei Dati
Raccogliere solo i dati adeguati, pertinenti e limitati a quanto necessario.

4. Esattezza
I dati devono essere esatti e aggiornati.

5. Limitazione della Conservazione
Conservati solo per il tempo necessario agli scopi del trattamento.

6. Integrità e Riservatezza
Trattati in modo da garantire sicurezza, protezione da trattamenti non autorizzati o illeciti.

7. Accountability (Responsabilizzazione)
Il titolare deve essere in grado di dimostrare la conformità ai principi.

CLASSIFICAZIONE DEI DATI

Dati Personali Comuni

- Nome, cognome, indirizzo
- Numero di telefono, email
- Data e luogo di nascita
- Codice fiscale

Dati Giudiziari

- Condanne penali
- Reati
- Misure di sicurezza

Dati Personali Particolari (ex "sensibili")

Richiedono protezione rafforzata:

- **Salute fisica o mentale**
- **Origine razziale o etnica**
- **Opinioni politiche**
- **Convinzioni religiose o filosofiche**
- **Appartenenza sindacale**
- **Dati genetici e biometrici**
- **Vita sessuale o orientamento sessuale**

Categorie Vulnerabili

Attenzione particolare per dati di:

- Minori
- Disabili
- Anziani
- Persone in stato di fragilità
-

BASI GIURIDICHE PER IL TRATTAMENTO

Per trattare dati personali serve almeno una base giuridica:

Consenso
dell'interessato (libero, specifico, informato, inequivocabile)

Contratto
(necessario per esecuzione contratto o misure precontrattuali)

Obbligo legale
(adempimento obblighi di legge)

Interesse vitale
(protezione vita dell'interessato o di terzi)

Interesse pubblico
(compito di interesse pubblico o esercizio pubblici poteri)

Interesse legittimo
del titolare o terzi (bilanciato con diritti interessato)

Per dati particolari: serve consenso esplicito o altre condizioni specifiche (es. finalità sanitarie, obblighi di legge).

RUOLI E RESPONSABILITÀ

Titolare del Trattamento

- Determina finalità e mezzi del trattamento
- Responsabile della conformità al GDPR
- Deve implementare misure tecniche e organizzative

Per associazioni: il Presidente o il Consiglio Direttivo

Responsabile del Trattamento (Data Processor)

- Tratta dati per conto del Titolare
- Deve avere contratto scritto con il Titolare
- Esempi: software house, società di hosting, consulenti esterni. Data Protection Officer (DPO)

Obbligatorio per:

- Pubbliche amministrazioni
- Trattamenti su larga scala di dati particolari
- Monitoraggio sistematico e regolare su larga scala

Compiti:

- Sorvegliare conformità GDPR
- Punto di contatto con Garante Privacy
- Formazione del personale

Per associazioni piccole: generalmente non obbligatorio, ma consigliato nominare un referente privacy.

MISURE TECNICHE E ORGANIZZATIVE

1. SICUREZZA FISICA

Controllo Accessi:

✓ Accesso limitato ai locali dove sono conservati dati Badge, chiavi, sistemi di controllo accessi

✓ Registro visitatori

✓ Armadi e cassetti chiusi a chiave per documenti cartacei ✓ Divieto di accesso a personale non autorizzato

Protezione Documenti Cartacei:

✓ Archiviazione in luoghi sicuri e chiusi

✓ Distruzione sicura (distruggi-documenti cross-cut)

✓ Limitare fotocopie e copie non necessarie

✓ Protocollo per smaltimento documenti

Esempio pratico - Associazione:

Documenti soci in archivio chiuso a chiave
Solo Presidente e Segretario hanno accesso
Registro di chi accede e quando
Distruzione annuale documenti oltre termini conservazione

2. SICUREZZA INFORMATICA

Protezione Dispositivi:

✓ Antivirus aggiornato su tutti i computer

✓ Firewall attivo

✓ Sistema operativo e software sempre aggiornati

✓ Backup regolari (giornalieri/settimanali)

✓ Crittografia hard disk (BitLocker, FileVault)

Controllo Accessi Logici:

✓ Account utente personali (no account condivisi)

✓ Password forti e cambiate periodicamente

✓ Autenticazione a due fattori (2FA)

✓ Blocco automatico schermo dopo inattività

✓ Disabilitazione account ex dipendenti/volontari

Gestione Password:

✓ Minimo 12 caratteri

✓ Maiuscole, minuscole, numeri, simboli

✓ Diversa per ogni servizio critico

✓ Uso di password manager aziendale e ambio password ogni 6-12 mesi

Protezione Rete: ✓ Wi-Fi protetto con WPA3 o WPA2

✓ Password Wi-Fi forte e riservata

✓ Rete ospiti separata per visitatori

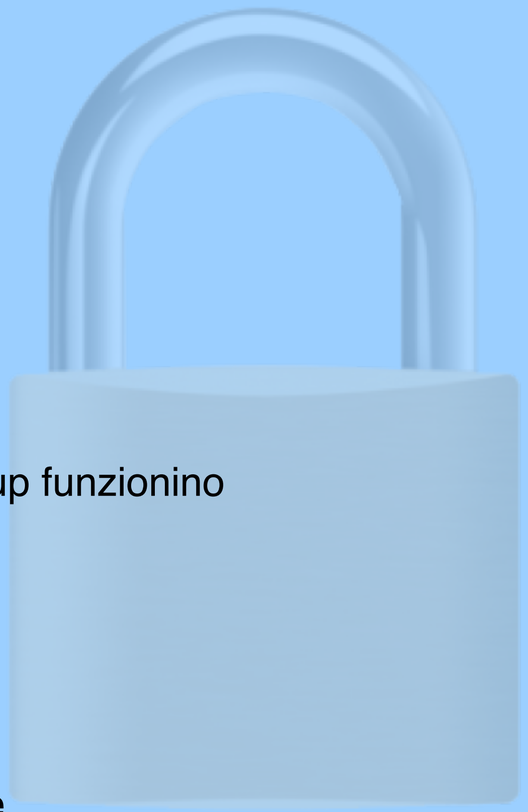
✓ VPN per accessi da remoto

✓ Segmentazione rete (separare dati sensibili)

3 BACKUP E DISASTER RECOVERY

Regola 3-2-1:

- **3** copie dei dati
- **2** supporti diversi (es. disco locale + cloud)
- **1** copia off-site (fuori sede)



Frequenza backup:

- **Dati critici:** giornaliero
- **Dati importanti:** settimanale
- **Archivi:** mensile

Test di ripristino:

✓ Verificare periodicamente (trimestrale) che i backup funzionino

✓ Simulare scenari di disaster recovery

✓ Documentare procedure di ripristino

Esempio - Associazione di medie dimensioni:

- Database iscrizioni: backup automatico ogni notte
- Documenti fiscali: backup settimanale
- Copia cloud crittografata su Google Drive Business
- Test ripristino ogni 3 mesi

CONSERVAZIONE E TEMPI DI RETENTION

Principio di Limitazione della Conservazione: i dati devono essere conservati solo per il tempo strettamente necessario.

DATI DEL PERSONALE:

- **Curriculum non selezionati:** massimo 2 anni (con consenso)
- **Dati dipendenti:** 10 anni dalla cessazione rapporto (obblighi fiscali)
- **Presenze e buste paga:** 10 anni
- **Infortuni sul lavoro:** illimitato (obbligo INAIL)

DATI FISCALI E CONTABILI:

- **Fatture, ricevute, documenti contabili:** 10 anni (D.P.R. 600/1973)
- **Dichiarazioni fiscali:** 10 anni
- **Libri contabili obbligatori:** 10 anni

DATI CLIENTI/SOCI:

- **Contratti attivi:** durata contratto + 10 anni (prescrizione ordinaria)
- **Dati marketing con consenso:** fino a revoca o 2 anni inattività
- **Soci associazioni:** durata iscrizione + tempi obblighi fiscali

DATI SANITARI:

- **Cartelle cliniche:** illimitato (obbligo deontologico)
- **Referti:** almeno 20 anni
- **Consensi informati:** durata trattamento + 10 anni

VIDEOSORVEGLIANZA:

- **Generalmente:** massimo 7 giorni (salvo necessità specifiche)
- **Con esigenze particolari:** fino a 30 giorni (motivato)

INFORMATIVA PRIVACY - Contenuto Obbligatorio (Art. 13 GDPR)
L'informativa deve essere: concisa, trasparente, intelligibile
Facilmente accessibile, **Linguaggio chiaro e semplice**

Deve contenere:
Identità e dati di contatto del titolare
Dati di contatto del DPO (se presente)
Finalità e base giuridica del trattamento
Legittimi interessi (se applicabile)
Eventuali destinatari dei dati
Intenzione di trasferire dati extra-UE
Periodo di conservazione
Diritti dell'interessato
Diritto di reclamo al Garante
Fonte dei dati (se non raccolti direttamente)
Eventuale processo decisionale automatizzato

Modalità di Rilascio
Momento: prima della raccolta dati
Formato: documento scritto (cartaceo o digitale), sito web (pagina dedicata), Email, modulo di registrazione.

Esempio
Modulo Iscrizione Associazione: INFORMATIVA PRIVACY (Art. 13 GDPR)
Titolare: Associazione XYZ, Via Roma 1, Castiglione del Lago (PG)
Email: privacy@associazionexyz.it
Finalità: gestione iscrizione, comunicazioni istituzionali, adempimenti fiscali
Base giuridica: esecuzione contratto associativo
Conservazione: durata iscrizione + 10 anni (obblighi fiscali)
Destinatari: solo personale autorizzato dell'associazione
Diritti: accesso, rettifica, cancellazione, limitazione, opposizione, portabilità
Per esercitare i diritti: privacy@associazionexyz.it
Reclami: Garante Privacy - www.garanteprivacy.it

☐ **Dichiaro di aver letto l'informativa privacy**
☐ **Acconsento al trattamento per invio newsletter (facoltativo)**