FORMAZIONE PRIVACY ai sensi dell'art. 29 GDPR

NESCA STUDIO LEGALE

- Dalla distanza di cortesia all'algoritmo
  la privacy a prova di Intelligenza Artificiale
- Lo stato del Regolamento a 6 anni dalla sua applicazione

Febbraio/Marzo 2023

Protezione dati, il Gdpr è ancora “incompiuto”: gli strumenti per garantirne la piena efficacia

A sei anni dalla sua entrata in vigore, non si può ancora parlare di applicazione efficace del Gdpr. La principale sfida per il futuro consiste nella necessità di procedere a un’integrazione degli strumenti giuridici propri di settori diversi quali quelli della concorrenza, data e consumer protection.

L’impatto del Gdpr e il futuro della data privacy

Il concetto di “applicazione efficace” del GDPR

I problemi che impediscono un’applicazione uniforme del GDPR

Il rapporto tra privacy e concorrenza

Le novità introdotte dal Digital Market Act

Convegno del Garante tenutosi il 24 maggio 2022
"25 anni di privacy in Italia – dalla distanza di cortesia all'algoritmo»

Link al filmato dell'evento

Ecco i punti focali su cui porre l'attenzione scaturiti dal convegno del Garante tenutosi il 24 maggio 2022 "25 anni di privacy in Italia" incentrato sui temi della protezione dei dati e PNRR, digitalizzazione, data economy e intelligenza artificiale:

- la dimensione digitale offre straordinarie opportunità ma pone il dovere di assicurare sempre, nei nuovi contesti, la tutela alla dignità della persona e alla sua sfera di riservatezza;
- il PNRR è un'occasione unica per la trasformazione digitale del Paese e mette a disposizione delle imprese e dei professionisti molte opportunità per una proficua "Transizione digitale" dei servizi che mette a disposizione dei propri clienti;
- la "digitalizzazione" dovrà essere la parola d'ordine per l'innovazione ma chiederà ad ogni impresa impegnata in progetti innovativi che passano attraverso i dati personali a considerarli sempre come un valore e mai come un mero strumento.

Il Piano Nazionale di Ripresa e Resilienza è un piano volto a supportare la ripresa economica del Paese dopo la pandemia da COVID-19 e a rafforzarne la resilienza in vista delle sfide future.

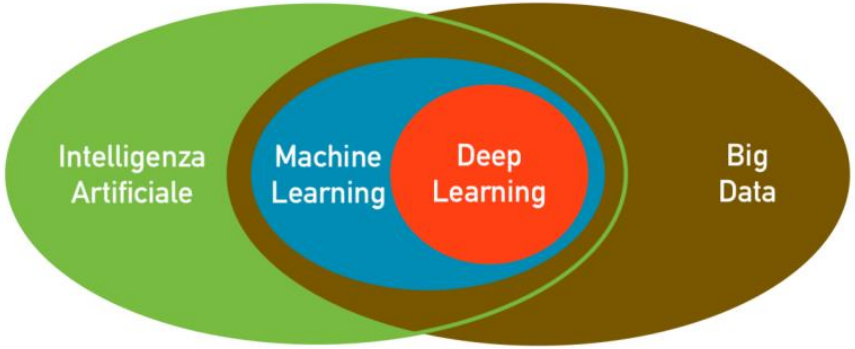
Il PNRR prevede una serie di misure per supportare le imprese nella transizione digitale, tra cui:

- Investimenti in infrastrutture digitali: il PNRR prevede la realizzazione di infrastrutture digitali di ultima generazione, come la banda ultra larga, per favorire la diffusione delle tecnologie digitali in tutto il Paese.
- Formazione e aggiornamento delle competenze digitali: il PNRR prevede la creazione di opportunità di formazione e aggiornamento delle competenze digitali per le imprese e i lavoratori, in modo da aumentare la loro capacità di utilizzare al meglio le tecnologie digitali.
- Agevolazioni fiscali e finanziamenti per l'adozione delle tecnologie digitali: il PNRR prevede la possibilità per le imprese di accedere a agevolazioni fiscali e finanziamenti per l'adozione delle tecnologie digitali.
- Promozione dell'innovazione e della collaborazione tra imprese: il PNRR prevede la promozione dell'innovazione e della collaborazione tra imprese attraverso la creazione di cluster e reti di imprese, in modo da favorire lo scambio di conoscenze e l'adozione delle tecnologie digitali.
- Inoltre, il PNRR prevede una serie di azioni per supportare le imprese nella transizione verso modelli di produzione e consumo sostenibili, come l'adozione di tecnologie a basso impatto ambientale e la promozione di pratiche di economia circolare.

In sintesi, il PNRR offre alle imprese diverse opportunità per promuovere la transizione digitale, sia attraverso l'adeguamento delle infrastrutture digitali sia attraverso la formazione del personale e l'innovazione.

Di seguito sono indicati i link per accedere alle agevolazioni e ai progetti promossi dalle azioni del governo:

https://www.mise.gov.it/it/incentivi



AI - Artificial Intelligence, è un campo di ricerca che studia come creare sistemi informatici in grado di simulare l'intelligenza umana.

1.L'obiettivo dell'AI è quello di sviluppare algoritmi e modelli che permettano ai computer di apprendere da dati e di compiere decisioni autonome basate su quelle conoscenze per questo i big data hanno un'importanza fondamentale per questo processo.

2.Il machine learning è una branca dell'AI che si concentra **sull'apprendimento di modelli statistici a partire da dati**.

3.Il deep learning, a sua volta, **è una tecnica di machine learning basata sulla creazione di reti neurali artificiali profonde**, **in grado di apprendere da dati di grandi dimensioni**.

4.La visione artificiale si occupa di sviluppare algoritmi in grado di **analizzare e comprendere immagini e video**, consentendo ai computer di "vedere" e di elaborare informazioni visive.

5.Il processing del linguaggio naturale è una tecnica di AI che si occupa dell'analisi e della comprensione del linguaggio umano, consentendo ai computer di elaborare testo, voce e linguaggio scritto.

6.La robotica è un campo di ricerca interdisciplinare che combina AI, ingegneria meccanica ed elettronica per **sviluppare robot capaci di svolgere compiti autonomamente.**

7.L'AI è una tecnologia in continua evoluzione e sta trovando applicazione in una vasta gamma di settori, tra cui la medicina, la finanza, l'industria manifatturiera, l'automazione degli uffici e molto altro ancora.

IL FENOMENO CHAT GPT

ChatGPT è un modello di linguaggio artificiale addestrato su enormi quantità di testo in diverse lingue, che gli permette di generare risposte ai messaggi in modo automatico. ChatGPT può essere utilizzato per conversazioni informali, domande e risposte, ricerca di informazioni e per generare testo in diversi stili e toni. Inoltre, ChatGPT può anche essere utilizzato per la traduzione automatica, la generazione di testo e la sintesi vocale, grazie alla sua conoscenza del linguaggio naturale.

L'acronimo GPT sta per "Generative Pre-trained Transformer", che significa "Trasformatore Generativo Pre-addestrato". È il nome della famiglia di modelli di linguaggio artificiale sviluppati da OpenAI, che includono ChatGPT e altri modelli di NLP (Natural Language Processing) avanzati.

https://chat.openai.com/chat

https://chrome.google.com/webstore/detail/chatgpt-chrome-extension/cdjifpfganmhoojfclednjdnnpooaojb

Il chatbot basato sull'intelligenza artificiale che è diventato virale, potrebbe **generare 1 miliardo di dollari di fatturato nel 2024.** Secondo tre fonti che hanno riferito a Reuters, il generatore di chatbot OpenAI vedrebbe le proprie entrate superare i 200 milioni di dollari nel 2023 e poi quintuplicare l'anno successivo.

Microsoft investe altri 10 miliardi in ChatGpt.
Microsoft studia come integrare OpenAI GPT in Office
https://www.ilsole24ore.com/art/microsoft-stregata-chatgpt-pronto-investimento-10-miliardi-AE14meVC?refresh_ce=1

PIATTAFORME AI PER AZIENDE

Ci sono molte piattaforme AI disponibili per le aziende. Qui di seguito un elenco delle migliori:

1.TensorFlow: è una delle librerie di machine learning più popolari e supportate dalla comunità. TensorFlow è utilizzato per la creazione di modelli di apprendimento automatico e reti neurali.

2.PyTorch: è un'altra libreria di machine learning molto popolare. PyTorch è apprezzato per la sua facilità d'uso e la sua flessibilità, in particolare per lo sviluppo di reti neurali.

3.Microsoft Azure: è una piattaforma di cloud computing che offre servizi di intelligenza artificiale e machine learning come parte della sua suite di strumenti per le aziende.

4.Amazon Web Services (AWS): è una piattaforma di cloud computing molto popolare che offre una vasta gamma di servizi AI e di machine learning, come Amazon SageMaker, Amazon Rekognition e Amazon Lex.

5.IBM Watson: è una piattaforma di intelligenza artificiale e machine learning che consente alle aziende di sviluppare soluzioni personalizzate utilizzando tecnologie come la computer vision, il processing del linguaggio naturale e la chatbot.

6.Google Cloud AI Platform: è una piattaforma di cloud computing che offre una vasta gamma di servizi di intelligenza artificiale e machine learning, come Google Cloud AutoML, Google Cloud Vision e Google Cloud Speech-to-Text.

7.H2O.ai: è una piattaforma di machine learning open source che offre un'ampia gamma di strumenti e librerie per lo sviluppo di modelli di machine learning, inclusi strumenti per la creazione di modelli di deep learning e reti neurali.

8.DataRobot: è una piattaforma di intelligenza artificiale e machine learning che consente alle aziende di creare e gestire modelli di machine learning complessi in modo automatico.

9.Microsoft Design AI è una piattaforma di strumenti e risorse per aiutare i designer a creare esperienze utente innovative e accessibili, utilizzando l'intelligenza artificiale. https://designer.microsoft.com/

La nuova versione di NVIDIA Broadcast permette di avere livestreaming e videoconferenze sempre più professionali, in particolare la nuova funzionalità Eye Contact
https://www.nvidia.com/it-it/geforce/broadcasting/broadcast-app/?ncid=afm-chs-44270&ranMID=44270&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-tAY7VduuRd6cTeiV1q.rRA

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Le PAROLE dell'AI

Il Garante racconta e spiega il rapporto tra Intelligenza Artificiale e protezione dei dati

www.gpdp.it/intelligenza-artificiale

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DEEPFAKE E DEEPNUDE

nelle parole di

GINEVRA CERRINA FERONI

Vice Presidente del Garante per la protezione dei dati personali

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ETICA E INTELLIGENZA ARTIFICIALE

nelle parole di

PASQUALE STANZIONE

Presidente del Garante per la protezione dei dati personali

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GLI ASSISTENTI DIGITALI

nelle parole di

AGOSTINO GHIGLIA

Componente del Collegio del Garante per la protezione dei dati personali

QUADRO DI RIFERIMENTO NORMATIVO

Attualmente il quadro normativo nazionale è definito dai seguenti provvedimenti:

1. **D.lgs 30/06/2003 Num. 196 - Codice in materia di protezione dei dati personali (con abrogazione e modifica di articoli con il D.lgs 101/2018)**

2. **Regolamento (UE) 2016/679 (GDPR) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.**

3. **DECRETO LEGISLATIVO 101/2018 del 10/08/2018 – Adeguamento nazionale al Regolamento UE 2016/679**

- I principi fondamentali del REGOLAMENTO (UE) 2016/679 (GDPR) e del DECRETO LEGISLATIVO 10 agosto 2018, n. 101

PROTEZIONE DEI DATI PERSONALI
Secondo i principi di liceità/finalità – minimizzazione

Il Regolamento UE

DATO PERSONALE

DATI COMUNI:

- l'insieme di dati che permette una identificazione dell'interessato
- *(nome, indirizzo, telefono, fotografie, email, conto corrente bancario, ...)*

DATI PARTICOLARI: dati che rivelano

- l'origine razziale o etnica
- le opinioni politiche
- le convinzioni religiose o filosofiche
- l'appartenenza sindacale
- dati genetici
- dati biometrici
- dati relativi alla salute
- dati relativi alla vita o orientamento sessuale

DATI PENALI: dati personali relativi a

- condanne penali
- reati
- dati connessi a misure di sicurezza

DATI ANONIMI:

- **informazioni che non possono essere associate ad un interessato identificato o identificabile, neanche tramite ricostruzione.**

A tali dati non si applica il Regolamento UE

Il Regolamento UE

TRATTAMENTO

NESCA STUDIO LEGALE

TRATTAMENTO

- **QUALSIASI** operazione o insieme di operazioni, compiute **con o senza l'ausilio di processi automatizzati** e applicate a dati personali o insiemi di dati personali, come *la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*

Dalla Raccolta → **Alla distruzione**

Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica:

- **consenso** (per **finalità relative a marketing** o che non rientrano nei fondamenti di seguito elencati)

altri fondamenti per cui non è necessario il consenso (a meno che non si trattino dati **particolari/sensibili/giudiziari)**

- **adempimento obblighi contrattuali**
- **interessi vitali della persona interessata o di terzi**
- **obblighi di legge cui è soggetto il titolare**
- **interesse pubblico o esercizio di pubblici poteri**
- **interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.**

Un'attenzione particolare va effettuata:

- al trattamento dei dati dei minori (Art.8 GDPR - in Italia l'età minima per non essere considerato minore per quanto riguarda il consenso per la privacy è 14 anni);

- al diritto dell'interessato di **non essere sottoposto a una decisione** basata unicamente **sul trattamento automatizzato e sulla profilazione** (Art. 22 GDPR) a meno che non venga espresso il consenso;

Cambridge Analytica e il furto di dati: "Così influenzavano le elezioni"

L'accusa è di avere rubato 50 milioni di profili da Facebook e di avere usato queste informazioni riservate per influenzare elezioni dall'America all'Europa, da Trump alla Brexit e oltre. Sul banco degli imputati c'è Cambridge Analytica, la società inglese di analisi di "big data" che da qualche anno ha ottenuto un'attenzione spropositata: c'è chi la ritiene il Grande Fratello orwelliano in grado di controllare il mondo

Confessa all'*Observer* l'autore della soffiata, Christopher Wylie: "Abbiamo sfruttato Facebook per raccogliere i profili di milioni di persone. E abbiamo costruito modelli per sfruttare quello che sapevamo su di loro e per prendere di mira i loro demoni interiori. Questa era la base su cui era fondata l'intera azienda". Una tecnica che gli esperti chiamano "psicografica".

"Usiamo dati per cambiare il comportamento dell'audience", afferma la homepage di Cambridge Analytica. mostrando alle organizzazioni non solo dove si trovano le persone, ma anche ciò a cui tengono veramente e cosa guida il loro comportamento.

Better audience targeting

Communication has changed. Blanket advertizing no longer provides viable ROI for every campaign. Big data revolutionized the way organizations identify and locate their best prospects. But data alone isnďž˝t enough. Cambridge Analytica is building a future where every individual can have a truly personal relationship with their favorite brands and causes by showing organizations not just where people are, but what they really care about and what drives their behavior.

Powered by smarter data modeling

At Cambridge Analytica we use data modeling and psychographic profiling to grow audiences, identify key influencers, and connect with people in ways that move them to action. Our unique data sets and unparalleled modeling techniques help organizations across America build better relationships with their target audience across all media platforms.

“UN MODO SICURO DI INDURRE LA GENTE A CREDERE A COSE FALSE È LA FREQUENTE RIPETIZIONE, PERCHÉ LA FAMILIARITÀ NON SI DISTINGUE FACILMENTE DALLA VERITÀ”

Daniel Kahneman

Premio Nobel per l'economia nel 2002 «per avere integrato risultati della ricerca psicologica nella scienza economica, specialmente in merito al giudizio umano e alla teoria delle decisioni in condizioni d'incertezza»

- I principi fondamentali del REGOLAMENTO (UE) 2016/679 (GDPR) e del DECRETO LEGISLATIVO 10 agosto 2018, n. 101

ORGANIZZAZIONE E RUOLI –PERSONE E COMPETENZE

Garante Privacy

D.P.O. – R.P.D. (Responsabile della protezione dei dati)

TITOLARE DEL TRATTAMENTO (Legale rappresentante dell'Ente/Azienda)

RESPONSABILI ESTERNI

SUB RESPONSABILI ESTERNI

Custode delle password-chiavi

Autorizzati al trattamento (Dipendenti)

Amministratore di Sistema

Responsabile del Sistema Informatico

INTERESSATI AL TRATTAMENTO

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**

c) informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

d) cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;

e) supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento** .

- I principi fondamentali del REGOLAMENTO (UE) 2016/679 (GDPR) e del DECRETO LEGISLATIVO 10 agosto 2018, n. 101

PROCESSI E REGOLE - DOCUMENTI

Privacy by Design e by Default
Accountability

Riferimenti normativi:
G.D.P.R
DLG 101 del 10/08/18

Documento con le misure di sicurezza aziendali

Misure di sicurezza degli edifici

Schema del Sistema informatico

Informativa e consenso (interessati al trattamento)

Registro delle attività di trattamento

Nomine di autorizzazione al trattamento (ex incaricati)

Nomine a amministratore di Sistema – responsabile del Sistema informatico – custode delle password/chiavi e istruzioni

Nomine a Responsabili esterni

Codice di Condotta
Codice etico
Codice deontologico

Analisi dei rischi

Valutazione di impatto (PIA)

Mappatura e inventario asset

- I principi fondamentali del REGOLAMENTO (UE) 2016/679 (GDPR) e del DECRETO LEGISLATIVO 10 agosto 2018, n. 101

SISTEMI DI CONTROLLO

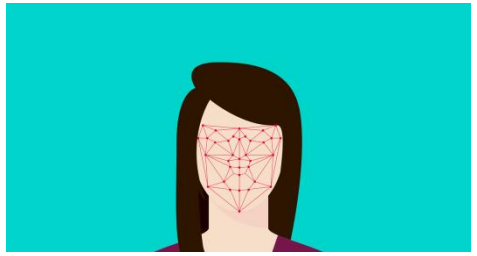
Registro archivi ad accesso controllato

Registro DATA BREACH (violazione dei dati)

Sistemi di Audit/Controllo rivolti ai responsabili esterni

Team privacy (Titolare - Consulenti esterni – D.P.O. – Amministratori di sistema e Responsabili del sistema informatico)

- Monitoraggio continuo del rispetto della normativa
- Scadenziario, verbali di aggiornamento annuale
- Formazione e informazione



E’ possibile installare gli impianti di videosorveglianza in azienda per finalità organizzative, produttive o di sicurezza **a condizione che vi sia un accordo preventivo con le Rappresentanze sindacali ovvero**, laddove non possibile, **che il Datore di Lavoro richieda una specifica Autorizzazione all’Ispettorato del Lavoro con compilazione e invio di un’istanza.**

Si ricorda che l’autorizzazione “preventiva” deve essere ottenuta prima dell’installazione dell’impianto di videosorveglianza e che sono potenzialmente soggette alla richiesta di autorizzazione tutte le imprese che hanno un impianto di videosorveglianza con registrazione e/o visione delle immagini che possano, **anche in via accidentale ed occasionale, generare possibilità di controllo a distanza dei lavoratori.**

Inoltre gli impianti di videosorveglianza, trattando dati, sono soggetti alle prescrizioni del GDPR si devono identificare gli “incaricati” alla visione delle immagini, esporre adeguate informative/cartelli e quello di limitare la conservazione delle registrazioni (max. 24/48 ore).

LA RECENTE CIRCOLARE DELL’INL N. 5 DEL 19 FEBBRAIO 2018 DISPONE CHE prima di procedere con l’installazione dell’impianto di telecamere si dovrà:

Verificare se tale installazione sia compatibile con i principi di liceità, di necessità, di proporzionalità e di finalità sanciti dal Codice della Privacy e sia compatibile con il divieto sancito dallo Statuto dei lavoratori.

Progettare l’impianto “a tavolino” con l’ausilio del progettista e/o dell’installatore professionista.

Predisporre il documento interno sulle motivazioni e la scelta della videosorveglianza nell’area aziendale, le misure minime di sicurezza, le informative. Conservare i log di accesso alle registrazioni per 6 mesi.

Qualora l’Azienda abbia già installato un impianto di videosorveglianza in assenza di autorizzazione sarà necessario disattivare l’impianto, coprire le telecamere e svolgere al più presto tutti gli adempimenti sopra indicati per non incorrere in sanzioni importanti.

Approfondimenti: Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014

Tali dati, per la loro peculiare natura, richiedono l’adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l’abusiva “ricostruzione” dell’impronta, partendo dal modello di riferimento, e la sua ulteriore “utilizzazione” a loro insaputa. L’utilizzo di dati biometrici dovrà, quindi, essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad “aree sensibili”, considerata la natura delle attività ivi svolte

Videosorveglianza: nel 92% dei casi le telecamere violano normativa sulla privacy

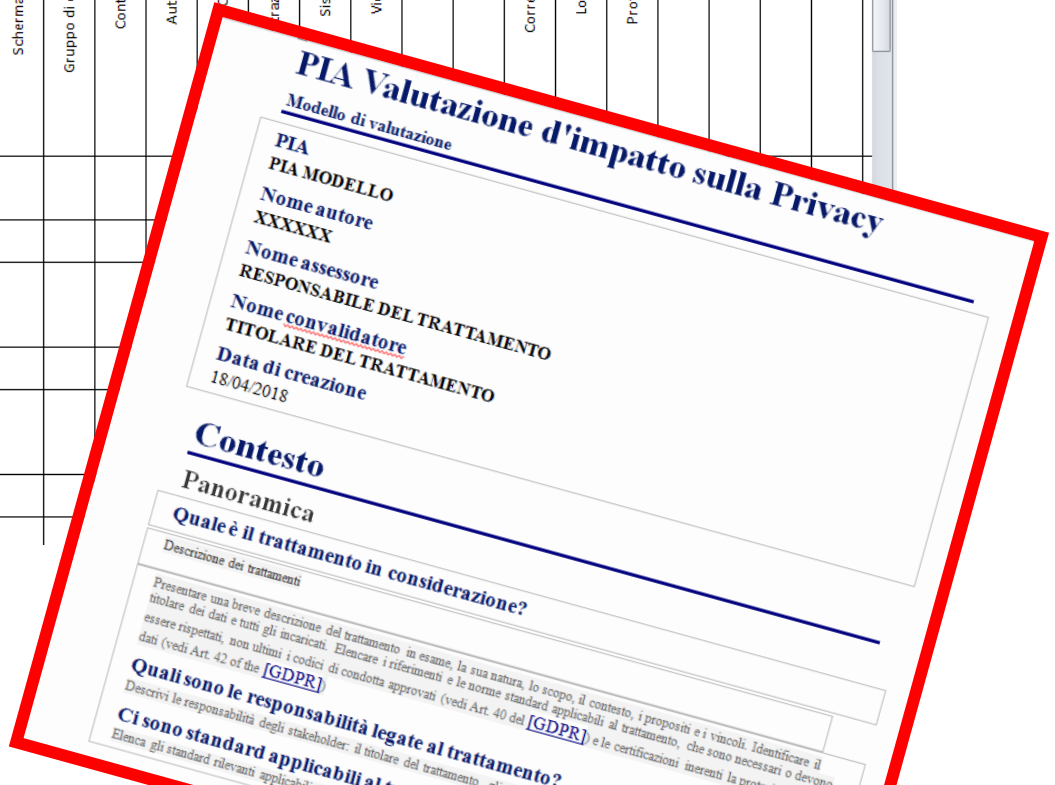
Uno studio realizzato da Federprivacy in collaborazione con Ethos Academy rivela che solo nell'8% dei casi i cittadini che entrano in un esercizio pubblico dotato di videosorveglianza trovano esposto un regolare cartello. Ammonta a oltre 4 milioni di euro il valore delle sanzioni per violazioni del GDPR dovuto a non conformità delle telecamere installate, il primato alla Spagna. Sono meno della metà i progettisti e gli installatori che si rendono conto dei reali rischi sulla privacy e del pericolo sanzioni

Addirittura, dallo studio è emerso che nel 38% dei casi non c'è proprio alcun cartello che mette a conoscenza il cittadino della presenza delle telecamere, e anche se nel restante 54% dei casi l'interessato prende atto che è esposto un cartello, tuttavia questo risulta non compilato con le informazioni necessarie o del tutto inadeguato a causa di riferimenti normativi obsoleti o sbagliati.

Analisi dei rischi
Valutazione di impatto (PIA)
Minimizzazione - Pseudonimizzazione

PRIVACY BY DEFAULT
PRIVACY BY DESIGN

Minaccia	Descrizione	ACCIDENTALE	DELIBERATA	AMBIENTALE	PROBABILITA' DEL RISCHIO (1-4)	GRAVITA' DEL RISCHIO (1-4)	VALUTAZIONE D'IMPATTO (PIA)	Protezione dei locali con serrature	Monitoraggio stato apparecchiature	Manutenzione periodica apparecchiature	Impianto di climatizzazione	Schermatura apparecchiature	Gruppo di continuità/stabilizzatore	Contenitori con chiave	Autenticazione utenti	Criptazione dati	...razione accessi ai locali	Sistema di allarme	Videosorveglianza	Backup dati	Assistenza	Corretta configurazione	Log file di accesso	Protocollo di rete SSL	Antivirus	Firewall	Formazione	Antispam
Uso non autorizzato dei dati	Abbandono della postazione senza effettuare la disconnessione dal sistema		x		2	3																					
Uso non autorizzato dei dati	Errata attribuzione dei diritti di accesso/credenziali	x																									
Uso non autorizzato dei dati	Smaltimento o riutilizzo dei supporti di memorizzazione senza una corretta cancellazione		x		1	4			x	x																	
Trattamento illecito dei dati	Abilitazione di servizi non necessari	x			2	3																					
Trattamento illecito dei dati	Mancate o insufficienti disposizioni in materia di sicurezza nei contatti con i clienti o terzi																										
Spamming o tecniche di sabotaggio	Mancanza di software antispam		x																								
Radiazioni elettromagnetiche	Sensibilità alle radiazioni																										



Esempio Check list di automonitoraggio MISURE DI SICUREZZA TRATTAMENTI				
N.	ADOTTATE	ADOTTARE	PIANO MIGLIORAMENTO	MISURA
				Controllo accessi a fotocopiatrici, stampanti e fax
				Custodia in armadi e cassetti provvisti di chiusura a chiave (procedura custodia)
				Custodia in cassaforte (limitazione accessi)
				Distruggi-documenti
				Pulizia scrivania
				Fotocopiatrice provvista di chiave/codice personale per ogni operatore
				Istruzioni incaricati – Codice di condotta
				Procedura gestione chiavi accesso ai locali
				Registro accessi ai documenti contenenti dati particolari e/o archivio storico
				Backup archivi e posta elettronica
				Crittografia (da adottare soprattutto per i dispositivi portatili)
				Firewall (a cura dell’amministratore di sistema)
				Firma digitale (uso controllato della firma)
				Manutenzione periodica della rete
				Presenza della nota confidenziale nei messaggi di posta elettronica
				Formazione del personale

Esempio Check list di automonitoraggio MISURE DI SICUREZZA TRATTAMENTI				
N.	ADOTTATE	ADOTTARE	PIANO MIGLIORAMENTO	MISURA
				Access log - Adottare LOG amministratore di sistema e ampliare esistenti
				Anonimizzazione dei dati
				Gruppo di continuità
				Manutenzione periodica hardware/inventario asset
				Manutenzione periodica software/inventario asset
				Prove periodiche ripristino backup
				Scheda segnalazione eventi dannosi / data breach
				Screensaver con password
				Sistema di autenticazione utenti (user e password complesse) custodia password
				Sistema di gestione dei privilegi utenti
				Software ati - virus
				Software anti-malware
				Badge controllo accessi
				Videosorveglianza
				Vigilanza

Registro dei trattamenti

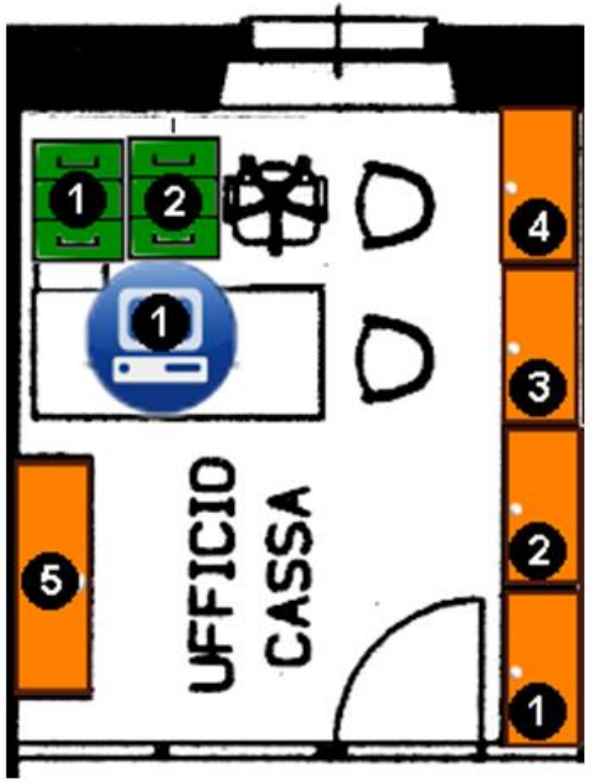
- Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trat- tamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

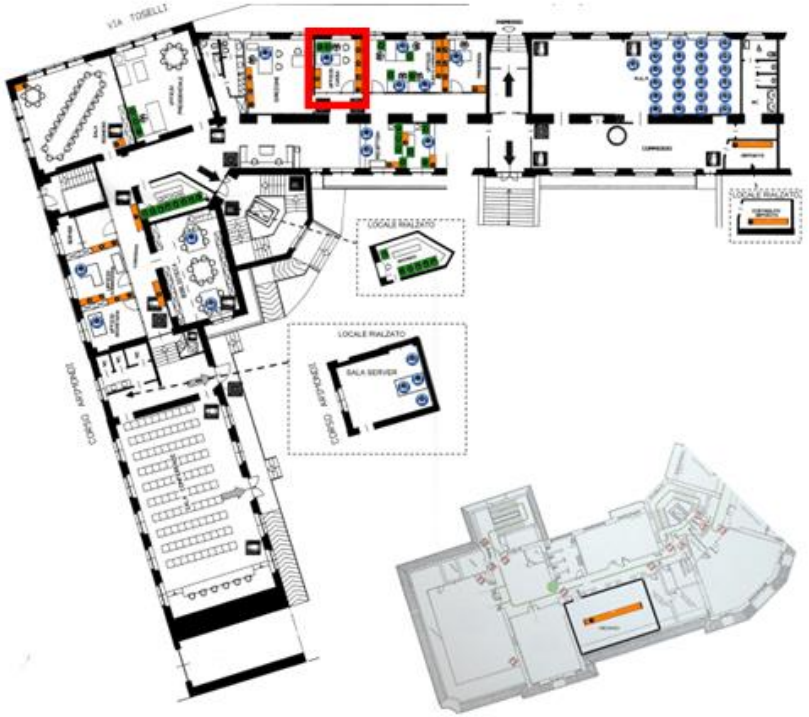
Raccomandazioni

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro

Registro dei trattamenti: mappatura asset

NOME DEL LOCALE/UFFICIO: **CONTABILITÀ**



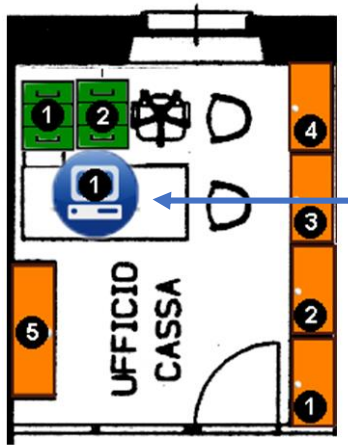


Registro dei trattamenti/asset

(CONSIGLIATA LA CONSERVAZIONE DIGITALE PER UN AGGIORNAMENTO CONTINUO)

Dati del TITOLARE o RESPONSABILE ESTERNO del TRATTAMENTO

Descrizione sintetica del trattamento	Natura dei dati C=dati comuni S=dati Sensibili G=dati giudiziari	Supporto C=cartaceo I=informatico	Interessati al trattamento esempio (Dipendenti/Clienti/Fornitori…)	Dati raccolti presso l'interessato? S=sì N=no - specificare la fonte	Specificare interesse legittimo e finalità (fare riferimento ad una legenda)	Altri destinatari del trattamento esterni all'azienda, eventualmente collocati in paesi UE e extra UE	Scadenza della conservazione dei dati per il trattamento (indicare la durata temporale riferita a obblighi di legge…)	Ufficio di riferimento (usare le sigle della mappa)	Tipologia di interconnessione e banca dati - indicare le sigle degli Armadi/Scaffali/Cassetti/Per i PC scivere ad esempio PC1 seguito da Rete Lan - Rete Wlan - PC Locale - segnare la banca dati corrispondente per i dati cartacei indicare FALDONE, DOSSIER, FASCICOLO, CARTELLINA, BUSTA... per i dati informatici specificare il percorso degli archivi su server o i dati di accesso al portale web, il software utilizzato	Nominativi degli autorizzati/incaricati	Livello gravità violazione dei dati 1=basso 2=medio 3=alto 4=alto+PIA
BUSTE PAGA DIPENDENTI	C S	C I	Dipendenti	S		- Azienda esterna elaborazione paghe STUDIO XXXXXXXX	10 anni	UFFICIO CASSA	A1 (CHIUSO A CHIAVE) DOSSIER PC1 SOFTWARE ZUCCHETTI	NOMINATIVO XXXXX	2



MISURE DI SICUREZZA DEGLI EDIFICI IN CUI VENGONO TRATTATI I DATI PERSONALI E CHE OSPITANO GLI ELABORATORI E GLI ARCHIVI CARTACEI E ARCHITETTURA DEL SISTEMA INFORMATICO

DATI DEL TITOLARE possiede i seguenti requisiti di sicurezza degli edifici.

Sede: INDICARE INDIRIZZO SEDE

Cancellare/modificare le righe o aggiungere altri criteri di sicurezza

La sede è dotata:

- ✓ di cancello di accesso alla struttura
- ✓ di porta pricipale blindata
- ✓ di inferriate per finestre
- ✓ di serrature a chiave delle porte interne
- ✓ di sistema di videosorveglianza dell'area esterna
- ✓ di sistema di videosorveglianza dell'area interna
- ✓ di impianto di allarme sonoro (collegato alle forze dell'ordine)
- ✓ di servizio di vigilanza notturno (ditta fornitrice: _____)
- ✓ di servizio di custode notturno
- ✓ di reception con controllo e registrazione degli accessi
- ✓ di incaricato alla custodia delle chiavi

Esiste un sistema di:

- ✓ prevenzione degli incendi con sistema di estintori secondo normativa (ditta fornitrice:_____)
- ✓ rilevazione dei fumi (ditta fornitrice:_____)
- ✓ presenza di idranti
- ✓ impianto di erogazione automatica di acqua in seguito a incendio (ditta fornitrice: _____)

Per i danni di tipo elettromagnetico degli elaboratori e per i danni dovuti a surriscaldamento:

- ✓ è presente un sistema di climatizzazione di tutti i locali
- ✓ è presente un sistema di climatizzazione nella sala server
- ✓ è presente un sistema di aerazione adeguato
- ✓ tutti i sistemi informatici sono dotati di gruppi di continuità UPS
- ✓ i sistemi server sono dotati di gruppi di continuità UPS

Per la protezione dei dati cartacei:

- ✓ l'accesso agli uffici ed alle banche dati è consentito solo ai dipendenti/personale incaricato
- ✓ gli archivi e i documenti cartacei sono riposti in armadi/scaffali/cassettiere non accessibili al pubblico
- ✓ i dati "particolari" sono conservati in armadi/cassetti chiusi a chiave con modalità di accesso selezionato e controllato

Aggiungere eventuali altre sedi con le caratteristiche di sicurezza

CARATTERISTICHE DEL SISTEMA INFORMATICO

PERSONALIZZARE L'ELENCO SEGUENTE

PD1 - SERVER:*

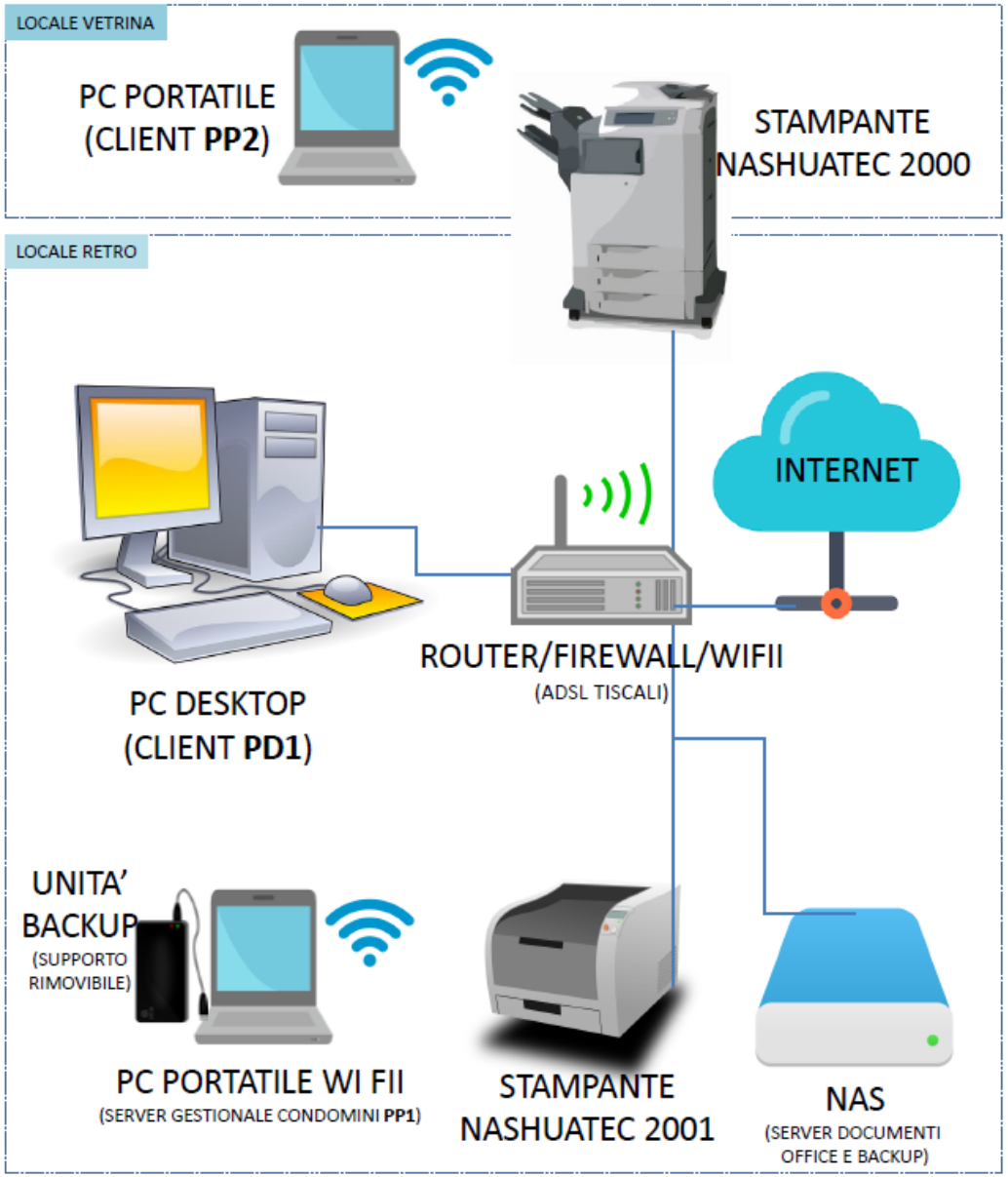
- Sistema INTEL CORE i3;
- Disco fisso di 450GB, RAM 4 GB
- S.O. Windows 8.1 con credenziali password di accesso alla rete informatica (user e password);
- aggiornamenti automatici patch di sicurezza del S.O.
- sistema antivirus certificato (aggiornamenti automatici on line);
- sistema di backup su supporto rimovibile e su server NAS (backup giornaliero a cura del titolare, conservazione del supporto rimovibile in luogo sicuro);
- software certificati installati:
  - suite Open Office (software open source)
  - programma "Gestionale…." (vedi scheda tecnica del fornitore ALLEGATO A10)
  - software scaricati da siti istituzionali per l'elaborazione di documenti da trasmettere on-line
- blocco PC con sistema di disconnessione (Ctr+Alt+Canc) e conseguente controllo accesso con user e password

PP1 - PC CLIENT:*

- Sistema INTEL CORE I3;
- Disco fisso di 439 GB, RAM 4 GB
- S.O. WINDOWS 8.1 con credenziali password di accesso alla rete informatica (user e password);
- aggiornamenti automatici patch di sicurezza del S.O.
- sistema antivirus certificato (aggiornamenti automatici on line);
- sistema di backup su supporto rimovibile e su server NAS (backup giornaliero a cura del titolare, conservazione del supporto rimovibile in luogo sicuro);
- software certificati installati:
  - suite Open Office (software open source)
  - programma "Gestionale…." (vedi scheda tecnica del fornitore ALLEGATO A10)

Esempio di schema del sistema informatico

Da completare a cura dell'amministratore di sistema o responsabile del sistema informatico



Informativa

Contenuti dell'informativa

- **I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13 e 14**

OGGETTO DEL TRATTAMENTO
I dati personali trattati sono raccolti verbalmente o mediante compilazione di moduli o formulari, anche con uso di strumenti informatici… raccolta di dati particolari
FINALITÀ DEL TRATTAMENTO
I dati da Lei forniti rientrano nel principio della liceità del trattamento per le seguenti condizioni e finalità…
MODALITÀ DEL TRATTAMENTO
I dati sono sottoposti a trattamento sia cartaceo sia elettronico e/o automatizzato.
Specificare il tempo di conservazione dei dati oggetto di trattamento oppure i criteri
Il trattamento non comporta o comporta (**in questo caso occorre il consenso**) processi decisionali automatizzati (profilazione).
CONFERIMENTO DEI DATI
Il conferimento dei dati è obbligatorio (fatta eccezione per le finalità di marketing)
COMUNICAZIONE DEI DATI AD ALTRI SOGGETTI
I Vostri dati possono saranno comunicati a terzi esclusivamente per esigenze strettamente collegate alle finalità indicate e in particolare alle categorie elencate qui di seguito:
TITOLARE – RESPONSABILE DEL TRATTAMENTO – AMMINISTRATORE DI SISTEMA
Specificare le figure
DIRITTI DELL'INTERESSATO
Nella Sua qualità di interessato, ha i diritti di cui al CAPO III del GDPR
MODALITÀ DI ESERCIZIO DEI DIRITTI
Potrà in qualsiasi momento esercitare i diritti inviando:

MANIFESTAZIONE DI CONSENSO AL TRATTAMENTO (art. 4 n. 11 e art. 7 del GDPR)
[necessario per marketing/profilazione/uso di immagini-video/dati relativi ai minori/dati particolari esclusi]

l'età per esprimere il consenso al trattamento dei dati personali del minore sia fissata in 14 anni sancito dal D.lgs. 101/2018 ; sotto tale soglia il trattamento dei dati personali del minore è lecito solo se il consenso sia stato prestato da chi esercita la responsabilità genitoriale

Diritti degli interessati

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

- Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), **1 mese**, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive.

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

- Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea.

Diritto di accesso (art. 15)

- Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento.

Diritto di cancellazione (diritto all'oblio) (art.17)

- Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Diritto di limitazione del trattamento (art. 18)

- Si tratta di un diritto esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati

Diritto alla portabilità dei dati (art. 20)

- Non si applica ai trattamenti non automatizzati il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Il termine inglese "accountabillity GDPR" significa **"operare con responsabilizzazione e dare prova di essere GDPR compliant"**.

Il principio di accountability attribuisce al titolare del trattamento un ruolo attivo e proattivo nel trattamento dei dati.
I soggetti accountable sono:

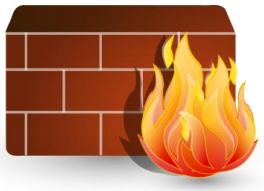
- **autonomi nelle decisioni** che prendono in merito al trattamento dati. Che non significa che sono soli: il titolare del trattamento può sempre nominare un DPO anche quando non è obbligatorio
- **rispondono direttamente delle decisioni** prese
- **hanno l'obbligo di rendicontazione**. Quindi devono dimostrare di aver agito in conformità al Regolamento, e che le misure intraprese sono efficaci per tutelare i dati.

- I principi fondamentali del REGOLAMENTO (UE) 2016/679 (GDPR) e del DECRETO LEGISLATIVO 10 agosto 2018, n. 101

STRUMENTI E TECNOLOGIE

Software e Hardware certificati e relazioni di conformità dei fornitori

Credenziali di accesso e lettera di incarico (regole su cambio password revoca aggiornamento)



Dotare i sistemi informatici di idonei strumenti di protezione (antivirus/firewall)

Sistemi di videosorveglianza e adempimenti

Pianificare backup dei dati e prove di ripristino

Armadi e locali provvisti di serratura

Richiedere relazioni sugli interventi effettuati dai tecnici/responsabili del sistema informatico

Protezioni particolari per dati sensibili

- Pseudonimizzazione
- Criptatura

Software e tecnologie di accesso remoto

Trasferimenti di dati verso Paesi terzi

- Il trasferimento di dati personali da paesi appartenenti all'UE verso Paesi "terzi" (non appartenenti all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è vietato, in linea di principio, a meno che il Paese in questione garantisca un livello di protezione "adeguato"

- In deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall'articolo 26, comma 1, della Direttiva 95/46 (consenso della persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, ecc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46).

Notifica delle violazioni di dati personali

- A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare** all'Autorità di controllo (Garante) le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessari. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione (**comunicazion**e) anche gli interessati, sempre "senza ingiustificato ritardo«.

Cos'è una violazione e quando va segnalata

Le violazioni dei dati personali possono essere accidentali – capitano per sbaglio o per errore - o volontarie, e sono:

1. **Accesso non autorizzato** (spionaggio se la violazione è volontaria) e si verifica se un terzo non autorizzato accede a dei dati personali.
2. **Copia non autorizzata** (furto se la violazione è volontaria) e si verifica quando un terzo non autorizzato ha copiato i dati dove non doveva.
3. **Divulgazione non prevista** (diffusione se la violazione è volontaria) e si verifica quando vengono diffusi dati personali che non dovevano essere divulgati.
4. **Modifica non autorizzata** (compromissione se la violazione è volontaria) e si verifica quando un terzo modifica dati che non poteva modificare.
5. **Perdita d'accesso** (cifratura se la violazione è volontaria) e si verifica quando i dati personali vanno persi.
6. **Cancellazione dei dati** (distruzione volontaria se la violazione è voluta) e si verifica quando viene cancellato il file che conteneva dati personali che erano salvati solo lì.

Le violazioni **vanno sempre documentate** nel registro, ma quando notificarle?
Il GDPR ci dice che vanno notificate entro 72 ore dal momento in cui se ne viene a conoscenza ma solo se la violazione può mettere a **rischio i diritti e le libertà degli interessati** (cioè le persone fisiche a cui appartengono i dati personali violati).

Perdita di:
- Reputazione
- Credibilità
- Ruolo
- Socialità
- Accesso a servizi

Conseguenze:
- Demansionamento
- Isolamento
- Pregiudizio
- Mancata erogazione di servizi
- Profilazione e condizionamento

Faldone Privacy

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 - DECRETO LEGISLATIVO 10 agosto 2018, n. 101	Allegato A0 Conservazione digitale
Nomine a Responsabili Esterni del trattamento	Allegato A1
Registro delle attività di trattamento	Allegato A2
Mappatura delle sedi e delle interconnessioni/asset	Allegato A3
Analisi dei rischi	Allegato A4
Valutazione di impatto (DPIA) ove richiesto	Allegato A5
Nomine di incarico di autorizzazione al trattamento(Art. 4.10 – Art. 28.b – Art. 29 GDPR)	Allegato A6
Nomina responsabile del sistema informatico, custode delle password, custode delle chiavi e altre nomine	Allegato A7
Codice di condotta per i soggetti autorizzati al trattamento dei dati personali (Art. 40 GDPR) e Altri Codici di condotta	Allegato A8
Altri codici di Condotta (Art. 40 GDPR)	Allegato A9
Provvedimento in materia di videosorveglianza - 8 aprile 2010 ed eventuale Documentazione relativa ai sistemi di videosorveglianza (ove prevista)	Allegato A10
Schede e dichiarazioni di adeguamento dei fornitori di prodotti software/hardware	Allegato A11
Misura di sicurezza degli edifici e dell'architettura di rete del sistema informatico/asset	Allegato A12
Interventi formativi e documentazione	Allegato A13
Informative e consenso al trattamento	Allegato A14
Aggiornamenti/Scadenze/Verbali	Allegato A15
Documentazione relativa ai Trasferimenti di dati personali verso paesi terzi o Organizzazioni internazionali (CAPO V GDPR)	Allegato A16

Nel lavoro agile in un'informativa il Titolare dovrà comunicare ai dipendenti i principali comportamenti da tenere e le tecnologie utilizzate.

Un valido suggerimento può essere quello dell'AGID che fornisce le seguenti **11 raccomandazioni per lo Smart Working sicuro**:

1. - Segui prioritariamente le policy, i codici di condotta e le raccomandazioni dell'Azienda
2. - Utilizza i sistemi operativi per i quali attualmente è garantito il supporto
3. - Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
4. - Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
5. - Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione
6. - Non installare software proveniente da fonti/repository non ufficiali
7. - Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
8. - Non cliccare su link o allegati contenuti in email sospette
9. - Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
10. - Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
11. - Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Le indicazioni appena elencate sono da ritenersi relative sia nel caso di utilizzo di dispositivi personali (situazione prevista dal noto paradigma BYOD) quanto nel caso di dispositivi configurati e forniti dall'Azienda.

IL DATORE DI LAVORO DEVE FORNIRE AL LAVORATORE I SUPPORTI TECNOLOGICI PER ATTUARE LE MISURE

Le regole per l'eventuale uso di dispositivi personali per l'attività lavorativa (BYOD).

Lo smartphone e il portatile sono tecnologie ormai indispensabili nella vita quotidiana, da cui i possessori non si separano neanche durante le ore di lavoro. Interpretando questa tendenza, le imprese e le scuole hanno cercato di approfittarne e il risultato è il BYOD, l'integrazione dei dispositivi personali sul posto di lavoro o a scuola.
Negli ultimi anni se n'è parlato tanto, spesso sottolineando i grandi vantaggi per le imprese, ma il BYOD ha anche i suoi difetti, soprattutto dal punto di vista della sicurezza informatica e della protezione dei dati. Per questo motivo, sono nate tendenze anche opposte al BYOD.
L'acronimo BYOD sta per Bring Your Own Device, che in inglese significa "porta il tuo dispositivo".
Ad esempio, con una politica di BYOD, un'azienda può permettere ai dipendenti di svolgere il lavoro sui propri computer e smartphone, in ufficio e al di fuori di esso.
Le policy di BYOD sono state sviluppate con il chiaro obiettivo di aumentare la produttività dei dipendenti e migliorarne (teoricamente) le condizioni di lavoro, partendo dall'idea che un lavoratore si sente più a suo agio utilizzando il proprio computer o i dispositivi che conosce meglio e usa tutti i giorni. Inoltre, l'applicazione del BYOD flessibilizza l'orario lavorativo e si adatta anche bene al lavoro agile.
Nel caso delle aziende, l'obiettivo è quello di ridurre i costi di proprietà dell'hardware e di gestione delle infrastrutture IT, aumentando contemporaneamente la produttività dei lavoratori.

Il BYOD non ha solo vantaggi e presenta alcuni inconvenienti sia a livello di gestione di IT sia a livello di sicurezza dei dati. Per questo motivo, l'introduzione del BYOD in un'azienda dovrebbe sempre essere accompagnata dalla creazione una politica di BYOD, anche conosciuta come policy BYOD o linee guida BYOD (**Per questo, il Garante Europeo della protezione dei dati (EDPS) ha pubblicato delle linee guida per il BYOD).**

In sintesi si dovrebbe:

- **Definire quali dispositivi possono essere utilizzati e come.**
- **Definire i sistemi e le procedure di sicurezza per il BYOD.**
- **Descrivere i rischi di sicurezza relativi ai dati personali.**
- **Definire le responsabilità giuridiche di azienda e dipendenti relative all'utilizzo dei dispositivi.**
- **Stabilire la gestione finanziaria della proprietà e dei dispositivi.**
- **Creare sui dispositivi personali container o spazi delimitati per l'utilizzo aziendale, a cui vengono applicate tecnologie di sicurezza particolari come il blocco di servizi di terze parti, cifratura**
- **Accesso a desktop virtuali e ambienti di lavoro basati sul web che consentono l'accesso remoto al PC aziendale dai dispositivi personali, mantenendo al sicuro i dati.**

Alternativa al BYOD
il corporate-owned, personally enabled (in italiano "di proprietà aziendale, abilitato per l'uso personale"), conosciuto come COPE.
Il metodo COPE ha i seguenti vantaggi rispetto al BYOD:
L'azienda sceglie i dispositivi, riducendo i problemi di compatibilità e di gestione.
L'azienda possiede i dispositivi, per cui può disporne come meglio crede per proteggere i dati e l'accesso alle reti aziendali.
In conclusione, non è chiaro quale sarà il futuro del BYOD, ma è sicuramente destinato a rimanere, almeno in una certa misura. La penetrazione dei dispositivi digitali nella vita di tutti i giorni sta cambiando il concetto stesso di rapporto lavorativo e i modi in cui viene svolto il lavoro. Resta da vedere quali metodi daranno i migliori risultati sia per le aziende che per i lavoratori.

Il tema della cybersicurezza per preservare i dati dal cybercrime e garantirne la conservazione e l'integrità; l'istituzione dell'Agenzia per la cybersicurezza nazionale (legge del 4 agosto 2021).

Clicca qui

https://threatmap.checkpoint.com/

https://www.webforma.it/news/top10-attacchi-informatici-primo-semestre-2021

Commissariato di P.S. online
Sportello per la sicurezza degli utenti del web

Che cosa prevede la nuova normativa italiana in tema di Cyber Security
È stata pubblicata in Gazzetta Ufficiale la **legge 4 agosto 2021, n.109 recante "Disposizioni urgenti in materia di cybersicurezza**, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" che converte il decreto legge 14 giugno 2021, n. 82.

Il Governo, attraverso l'approvazione della legge, intende promuovere la cultura della sicurezza cibernetica e aumentare la consapevolezza sul tema all'interno del settore pubblico e privato, **accendendo i riflettori sui rischi e sulle minacce cyber**.

Negli ultimi anni, infatti, l'accresciuta esposizione alle minacce cibernetiche ha evidenziato la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela e Cyber Security: nessun settore è immune da possibili cyber attacchi: **solo nel 2020, infatti, sono stati registrati 1.871 gli attacchi gravi di dominio pubblico, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica**.

Il pool di esperti che ha lavorato alla stesura del rapporto pone l'accento sull'incremento degli attacchi cyber a livello globale, che nel 2020 è pari a un +12% rispetto al 2019, e sull'aumento degli attacchi gravi con un +66% rispetto al 2017.

Tra i settori maggiormente colpiti ci sono il "Multiple Targets" (20% del totale degli attacchi), che comprende attacchi realizzati verso molteplici obiettivi spesso indifferenziati, il settore Governativo, militare, forze dell'ordine e intelligence (14% del totale degli attacchi), la sanità, (12% del totale degli attacchi), la ricerca e istruzione (11% del totale degli attacchi) e i servizi online (10% del totale degli attacchi). Inoltre, sono cresciuti gli attacchi verso Banking & Finance (8%), produttori di tecnologie hardware e software (5%) e infrastrutture critiche (4%).

In una società sempre più digitale, dove cresce il fenomeno della Gig Economy ed è impossibile fare a meno della tecnologia, quello della Cyber Security è uno dei temi più rilevanti dell'agenda nazionale ed internazionale.

La Cyber Security quindi è l'insieme dei mezzi, delle tecnologie e delle procedure utili a proteggere i sistemi informatici in termini di disponibilità, riservatezza e integrità dei dati e degli asset informatici. La cyber sicurezza costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021. Inoltre, è uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione.

L'investimento, che mira alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese, interessa quattro diverse aree:

1. **Rafforzamento dei presidi di front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse nazionale;**
2. **Consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'hardware e del software;**
3. **Potenziamento del personale delle forze di polizia dedicate alla prevenzione e investigazione del crimine informatico;**
4. **Implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.**

I principali compiti dell'Agenzia sono:

- Promuovere la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni;
- Predisporre la strategia nazionale di cybersicurezza;
- Svolgere ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza;
- Sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione, per far fronte agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il Computer Security Incident Response Team (CSIRT) italiano e l'avvio operativo del Centro di valutazione e certificazione nazionale;
- Curare e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale;
- Contribuire all'innalzamento della sicurezza dei sistemi di Information and communications technology (ICT) dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, delle pubbliche amministrazioni, degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD);
- Supportare lo sviluppo di competenze industriali, tecnologiche e scientifiche, promuovendo progetti per l'innovazione e lo sviluppo e mirando a stimolare nel contempo la crescita di una solida forza di lavoro nazionale nel campo della cybersecurity in un'ottica di autonomia strategica nazionale nel settore.

1. **Creare un inventario**
2. **Individuare i sistemi critici.**
3. **Nominare un responsabile del sistema informatico.**
4. **Conoscere i regolamenti (attenersi al Codice di Condotta aziendale sulla privacy)**
5. **Formare il personale.**
6. **Fare attenzione al lavoro da remoto.**
7. **Installare antivirus.**
8. **Aggiornare software.**
9. **Fare più backup in «panieri diversi».**
10. **Stabilire una policy per le password.**
11. **Limitare i servizi web offerti da terzi.**
12. **Non condividere dati delicati all'esterno.**
13. **Controllare l'uso dei supporti rimovibili.**
14. **Proteggere con Firewall.**
15. **Non aprire link nelle email.**
16. **Policy BYOD e smart working.**
17. **Non cliccare sui pop up.**
18. **Proteggere il sito web.**
19. **Fare acquisti solo su siti sicuri.**
20. **Schermare la cam.**
21. **Controllare i post sui social media.**

PERCHÉ GLI HACKER VOGLIONO I TUOI DATI PERSONALI?

1. Gli hacker possono **vendere i tuoi dati ad altri criminali**
Un modo in cui gli hacker lucrano sui dati rubati è rivenderli in massa ad altri criminali nel dark web. Queste raccolte includono milioni di record di dati rubati. I compratori possono usare questi dati per i propri scopi illeciti.

2. I dati personali sono alla base dei **furti di identità**
Il furto di identità è un crimine in cui i dati personali delle vittime vengono usati per ottenere vantaggi a loro spese. Molti servizi online richiedono agli utenti di inserire i propri dati personali come nome, indirizzo e numero della carta di credito. I criminali rubano questi dati dagli account online per commettere furti di identità, ad esempio utilizzando la carta di credito della vittima o chiedendo prestiti a loro nome.

3. **I dettagli di accesso sono necessari per impadronirsi di un account**
I criminali usano le credenziali di accesso rubate per introdursi negli account con dettagli di pagamento, ad esempio quelli di shopping. Si impadroniscono di fatto dell'account, cosa che spesso porta al furto di identità. Se l'hacker cambia la tua password, non potrai più nemmeno accedervi. Questa situazione può essere costosa se l'account includeva dettagli di pagamento.

4**. I dati sottratti vengono usati per effettuare attacchi di phishing ed estorsioni mirati**
Con queste informazioni personali rubate, i criminali possono scegliere con più precisione le vittime degli attacchi di phishing. In queste truffe, le vittime vengono convinte a fornire informazioni come dati delle carte di credito a criminali che si spacciano per enti legittimi. Se i criminali ottengono accesso a dati molto sensibili, potrebbero anche chiedere riscatti alla vittima.

5. **I dati personali rubati possono essere usati per fare un danno alle aziende**
Oltre ai problemi personali, questi furti possono danneggiare anche le aziende. Con i dati sottratti, i criminali possono convincere il personale a fornire dati sensibili o a effettuare pagamenti. Tali attacchi di phishing a un individuo specifico sono detti attacchi di "spear-phishing". I criminali possono anche provare a ottenere l'accesso alle reti aziendali per spiarle e infettarle con malware.

Privacy Policy: cosa cambia nel 2022 e come aggiornare il sito

Dal 10 gennaio 2022 i siti web devono rispettare le nuove "Linee Guida sui Cookie ed altri strumenti di tracciamento".
Ecco come aggiornare il sito

Gestione cookie: regole da seguire dal 2022

Le **linee guida** attive a partire dal 2022 sono dedicate a una particolare attività, ovvero la gestione dei **cookie** e altri **strumenti di tracciamento**. I cookie non sono tutti uguali, ma cambiano in base al sito web che li utilizza e ai dati che desiderano ottenere dall'utente. Iniziamo col dire che sono stringhe di testo che una piattaforma invia a un utente e che vengono installate nel suo dispositivo. Vediamo quali sono le tipologie di cookie, l'obiettivo e a quali regole devono sottostare.

I **cookie tecnici** sono detti "necessari" e vengono usati per permettere all'utente di compiere una determinata azione su un sito. A partire dal 2022 per usare queste stringhe bisognerà informare l'utente, ma non sarà necessario avere il suo consenso.

I **cookie analitici**, al contrario, sono quelli utilizzati da un sito per analizzare il traffico e l'utenza. Possono essere rilasciati dietro adeguata informativa e senza chiedere il consenso, ma solo ad alcune condizioni:

- se vengono usati a scopi statistici
- nel caso siano cookie di terze parti per i quali è nascosta una parte dell'indirizzo IP
- se le terze parti non trasmettono dati all'esterno e non li combinano

Per utilizzare cookie di diverso tipo sarà necessario richiedere il **consenso dell'utente**.

Ci sono, poi, i **cookie di profilazione** che sono usati per studiare preferenze dell'utenza e offrire **prodotti e servizi personalizzati**. In base a questi codici vengono inviati **specifici messaggi pubblicitari** perchè captano le **preferenze dell'utente durante la sua navigazione online**. Su questi elementi occorre fare molta attenzione, perchè di fatto sono quelli che possono potenzialmente invadere la **privacy dei consumatori**. In base alle nuove Linee Guida, per utilizzarli è necessario ottenere il **consenso** prima che il cookie venga installato nel suo dispositivo. Oltre a questo è necessario fornire l'**informativa breve per i Cookie Banner** e l'**informativa estesa per la Cookie Policy**.

GDPR 2022: cos'è il consenso e come si ottiene

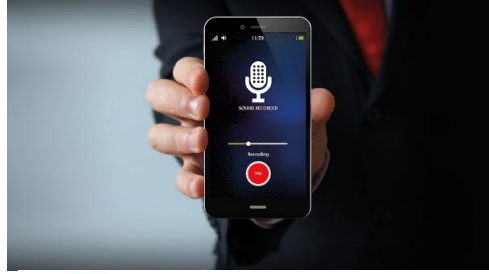
Con le nuove regole, appare chiaro che ottenere il concetto di "consenso" diventa cruciale. **Ma cos'è il consenso e quando è necessario?** Innanzitutto, il Garante deve assicurarsi che qualsiasi raccolta e archiviazione di informazioni personali sia eseguita con l'approvazione dei diretti interessati, in particolare quando si vuol profilare un comportamento. Non è possibile raccogliere i dati motivandoli col "legittimo interesse" del titolare del sito web.

Il consenso deve avere **specifiche caratteristiche**:

- deve essere **dato liberamente** dall'utente e non deve essere estorto. Per esempio, non si può ostacolare l'utilizzo di un sito web prima che l'utente abbia flaggato la casella dei cookie, ma questa non deve impedire l'accesso e l'uso di piattaforme
- deve essere **specifico** e deve permettere all'utente di comprendere subito qual è l'obiettivo del sito web e, nel caso di differenti cookie, si devono capire le differenti finalità
- deve essere **chiaro** e comunicato in modo **inequivocabile**, sono vietate alcune pratiche poco trasparenti, come i form pre-flaggati.

Se i siti web non rispettano queste caratteristiche risultano illegittimi e possono essere sottoposti a penali e sanzioni. I **siti web** che ancora non hanno adattato le proprie policy devono adeguarsi il prima possibile.

E’ lecito registrare una telefonata? Ecco cosa prevede il Codice Privacy



Registrare una conversazione all’insaputa dei presenti

È lecito registrare una conversazione che si intrattiene tra più persone ed all’insaputa di tutti o solo di alcuni. Chi parla accetta anche il rischio di essere registrato, dice la Cassazione. È però necessario che:

- alla conversazione partecipi colui che sta registrando, non ci può limitare a lasciare un sistema di registrazione e non essere presente;
- la registrazione non avvenga nei luoghi di privata dimora del «registrato», è illegale andare a casa di un amico o nel suo ufficio riservato e attivare la registrazione; bisognerebbe trovarsi in un luogo pubblico per attivare la registrazione
- é invece possibile registrare in casa propria quello che dicono invece gli ospiti.

Registrare una telefonata all’insaputa dell’altro

Così come è legale la registrazione di una conversazione tra presenti e all’insaputa di questi, la registrazione di una telefonata con un’altra persona ignara di essere “intercettata” non viola l’altrui privacy e, quindi, non costituisce reato.

Questo perché, secondo la Cassazione, la registrazione non fa che fissare, su una memoria elettronica, ciò che è già “nostro” e fa parte del nostro patrimonio sensoriale, essendo stato captato dal nostro udito e immagazzinato nella nostra memoria

Tale è stato anche l’orientamento espresso dalle Sezioni Unite della Cassazione nella famosa sentenza “apripista” del 2003 secondo cui la registrazione del colloquio, in quanto rappresentativa di un fatto, integra la prova documentale.

Posso far sentire ad altri o pubblicare la conversazione telefonica?

Se è legale registrare una telefonata, non lo è invece la pubblicazione del suo contenuto. Non si può quindi far ascoltare l’audio a una platea di uditori (ad esempio nel corso di una riunione di condominio), non si può pubblicare il file su internet o su un social network (a meno che si distorca il suono in modo da non far risalire all’autore della dichiarazione e vengano oscurati eventuali altri nomi citati nella conversazione). La legge vieta infatti solo la diffusione della conversazione salvo ci sia il consenso di tutti coloro che vi hanno partecipato (e non solo di uno).

Resta chiaramente lecito far sentire il contenuto della registrazione telefonica a un giudice, a un carabiniere, a un poliziotto e a qualsiasi altra autorità preposta alla tutela dei diritti del cittadino.

Ad esempio, è possibile fa ascoltare il file nel corso di un procedimento disciplinare dinanzi al proprio datore di lavoro; in una causa di separazione o divorzio per dimostrare, ad esempio, l’altrui confessione di tradimento; o in un giudizio per il recupero di un credito, per provare l’ammissione del debitore.

Sembrerà strano ma è proprio il Codice della Privacy a consentire la registrazione di una telefonata eseguita all’insaputa dell’altro conversante. Ciò infatti è necessario “per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento”.

Si può registrare una videoconferenza?

Le stesse regole previste per il telefono o lo smartphone valgono anche per le video conferenze. È lecito quindi registrare una chiamata via Skype o con qualsiasi altra applicazione per i video messaggi, fosse anche WhatsApp, Messenger, Zoom o altri.

Obbligo FORMATIVO per tutte le componenti

Articolo 29 GDPR

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati **se non è istruito** in tal senso dal titolare del trattamento

p.s. per il personale assente durante la formazione é opportuno attivare modalità di autoformazione/comunicazione per tali soggetti

Sanzioni CAPO VIII GDPR – Artt. 77-84

Il Gruppo di lavoro Articolo 29 ha adottato delle **Linee Guida** sui criteri di valutazione dell' apparato sanzionatorio.

Sulla base dell'**art. 82 del GDPR** l'interessato che subisca un danno materiale o immateriale può ottenere il risarcimento del danno.

Le sanzioni amministrative possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi di, a titolo esemplificativo:
- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza.

possono salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nei casi di, a titolo esemplificativo:
- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito di dati personali in un Paese terzo.

la determinazione della sanzione verrà valutata da:
- "la natura, gravità e durata della violazione";
- "il carattere doloso o colposo della violazione";
- "il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi".

Si dovrà definire il carattere colposo o **doloso. Ipotesi di carattere doloso potranno essere**:
- trattamenti illeciti autorizzati dal titolare ignorando i pareri formulati dal DPO;
- modifica di dati personali, avente la finalità di fornire un'impressione "fuorviante";
- vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Controlli del nucleo operativo privacy della GDF sulla base di controlli ordinari o segnalazioni al Garante.

SUGGERIMENTI E CONSIDERAZIONI

Come nasce un'ispezione

a seguito di segnalazioni o reclami dei soggetti interessati oppure su iniziativa del Garante, per conoscere lo stato di attuazione della normativa in determinati settori pubblici e privati.

se un'organizzazione ha già ricevuto richieste di informazioni da parte dell'Autorità, questo potrebbe comportare un aumento della probabilità di ricevere una "*visita di persona*".

La probabilità aumenta ancora di più se le richieste di informazioni si riferiscono all'ambito oggetto del piano semestrale del Garante.

Le attività ispettive

sono condotte dal Nucleo Speciale Privacy della Guardia di Finanza. Nei casi più gravi e in cui sono richieste competenze specifiche maggiori, funzionari del Garante

procedono personalmente alle ispezioni con o senza il supporto della GdF. *Pertanto, sempre in linea generale, laddove l'ispezione sia condotta in prima persona da funzionari del Garante, è legittimo aspettarsi che l'Autorità consideri che la situazione sia già controversa, in tema di rispetto della normativa sulla protezione dei dati personali.*

L'ispezione potrebbe portare a una ulteriore emersione di possibili violazioni in materia.

Le ispezioni possono essere "**annunciate**" dal Garante o dalla GdF tramite una comunicazione (spesso solo il giorno prima dell'arrivo) ma possono anche avvenire "**a sorpresa**":

Nel primo caso, è opportuno che chi controlla la PEC dell'organizzazione si renda conto della serietà della questione e avverta subito i vertici e noi in modo da prepararsi all'arrivo degli ispettori.

Quale che sia il tipo di ispezione, il perimetro dell'ispezione è individuato da un documento che viene notificato al momento dell'accesso in sede: si tratta della ***"richiesta di informazioni"*** con cui il Garante domanda come siano stati assolti determinati obblighi legislativi o regolamentari in materia di protezione dei dati personali.

La richiesta di informazioni, per esempio, può includere come venga data l'informativa agli interessati, come venga raccolto il consenso ove necessario, come vengano contrattualizzati i responsabili esterni del trattamento, quali misure di sicurezza siano applicate, per quanto tempo e come vengano conservati i dati trattati ecc. se al momento non vi viene notificato nulla, potrete rifiutarvi di fornire qualsiasi informazione sino a quando non conoscerete l'oggetto dell'ispezione.

Ispezioni del Garante Privacy: suggerimenti pratici per le aziende
Avere una procedura interna affinché siano avvisati i vertici dell'organizzazione e siano già individuati i soggetti preposti alla gestione degli ispettori:
il responsabile privacy (ove non sia stato nominato il DPO o ove il DPO sia assente);
i consulenti privacy + lo studio legale legale.
il punto d'ingresso su cui indirizzare gli ispettori è normalmente il registro dei trattamenti che deve **OVVIAMENTE** essere aggiornato;

Lo scopo è di evitare risposte evasive e poco circostanziate e la possibilità di rimettersi ad una documentazione esaustiva evitando così errori o incomprensioni.

A proposito di risposte.
E' importante controllare e verificare la verbalizzazione di quello che avviene e delle dichiarazioni di cui si desidera lasciare traccia.
E' essenziale sempre riservarsi di verificare la correttezza di quanto dichiarato, anche al fine di limitare i rischi di sanzioni.

E' consigliabile che le dichiarazioni a verbale siano vagliate dal legale e/o consulente privacy in modo da verificare che non si rivelino controproducenti o contraddittorie.

A prescindere dalla verbalizzazione, nell'interlocuzione con gli ispettori, **ove non si sia sicuri** di qualcosa è bene attendere e **riservarsi di rispondere successivamente**.

- Gli ispettori potrebbero essere verosimilmente interessati alla produzione di documentazione rilevante ai fini dell'accesso (informative, contratti, policy ecc.). ERGO più completa ed esaustiva è il "fascicolo privacy" maggiore sarà la possibilità di soddisfare le richieste dell'Autorità.

In ogni caso, **tipicamente sono assegnati 15 giorni (dalla notificazione della richiesta di informazioni e quindi dal primo giorno di ispezione) per l'invio di copia della documentazione richiesta**. Pertanto, il mancato soddisfacimento immediato di una (parte della) richiesta dell'Autorità è qualcosa che accade di frequente.

È consigliabile che almeno una delle persone individuate per la gestione dell'ispezione sia presente per tutto il tempo in modo da coordinare i lavori e fare da punto di riferimento sia interno che per gli ispettori.

A fine giornata (di solito le ispezioni durano 2-3 giorni) è consigliabile che venga svolto un report interno di cosa è successo, allegando anche copia del verbale e, ove possibile, cosa accadrà l'indomani.

Ulteriori cautele:

- non rilasciare mai documentazione in originale ma solo copie;
- prendere nota di tutti i documenti (inclusi anche banche dati, archivi, software)visionati dagli ispettori e delle informazioni richieste e fornite;
- farsi rilasciare copia del verbale;
- dimostrarsi collaborativi e non reticenti;
- rilasciare sempre informazioni veritiere e corrette (nel dubbio, non rispondere e riservarsi è meglio che dare informazioni false).
- In caso di richiesta di documentazione riservata, è consigliabile verificare di anonimizzare o cancellare le parti che non si desidera mettere a disposizione dell'Autorità (per esempio, i termini economici di un accordo). Ciò dimostrerà anche che il nostro sistema privacy funziona.