Privacy aziendale: guida sintetica per le imprese

INDICE – Privacy aziendale: guida sintetica per le imprese

I dati

La privacy aziendale è un tema di crescente importanza in Italia. I dati personali sono diventati una risorsa preziosa per le imprese, ma al contempo è fondamentale garantire la loro adeguata protezione. Secondo i dati più recenti, le violazioni della privacy aziendale sono in aumento, con gravi conseguenze per le aziende coinvolte. In Italia, le leggi che disciplinano la privacy includono il Regolamento Generale sulla Protezione dei Dati (GDPR) e il Codice della Privacy, che stabiliscono i diritti e gli obblighi delle imprese in materia di trattamento dei dati personali. Le sanzioni per violazioni della privacy possono essere significative, con multe che possono arrivare fino al 4% del fatturato annuale dell'azienda. È fondamentale che le aziende si conformino alle

leggi sulla privacy, implementando adeguate misure di sicurezza e rispettando i diritti dei titolari dei dati.

Privacy aziendale: rispetto delle regole GDPR

“Proteggere insieme i tuoi dati, un tesoro da preservare” è lo slogan adottato dal Garante per la protezione dei dati personali in una delle sue campagne pubblicitarie, sottolineando l’importanza della protezione dei dati dopo l’entrata in vigore del Regolamento Generale sulla Protezione dei Dati (GDPR).

Il GDPR ha notevolmente contribuito a rendere la protezione dei dati personali un pilastro fondamentale del nostro sistema normativo. La sua ampia portata implica che ogni azienda e professionista, salvo rare eccezioni, debba rispettare le disposizioni del Regolamento stesso e delle normative nazionali (come il d.lgs. n. 196/2003, modificato dal d.lgs.

n. 101/2018).

Nonostante siano trascorsi diversi anni dall'entrata in vigore del GDPR, molte imprese non hanno ancora completato o addirittura iniziato il processo di adeguamento. Ciò comporta notevoli rischi in termini di impatto diretto sulle attività aziendali e di possibili violazioni amministrative e penali, con conseguenti sanzioni significative.

Adeguamento GDPR e privacy: una sintesi per le imprese

Per adeguarsi al GDPR e alla normativa sulla privacy, è necessario seguire un processo articolato. Di seguito sono indicate le fasi principali:

1. Analisi dell'azienda e individuazione delle attività di trattamento dei dati.

2. Valutazione dei rischi e implementazione di adeguate misure di sicurezza.

3. Nomina, se necessario, di un Responsabile per la protezione dei dati (DPO o RPD).

4. Creazione dell'Informativa Privacy per gli interessati.

5. Definizione dei ruoli e disciplina dei rapporti con i soggetti coinvolti.

6. Redazione del Registro delle attività di trattamento.

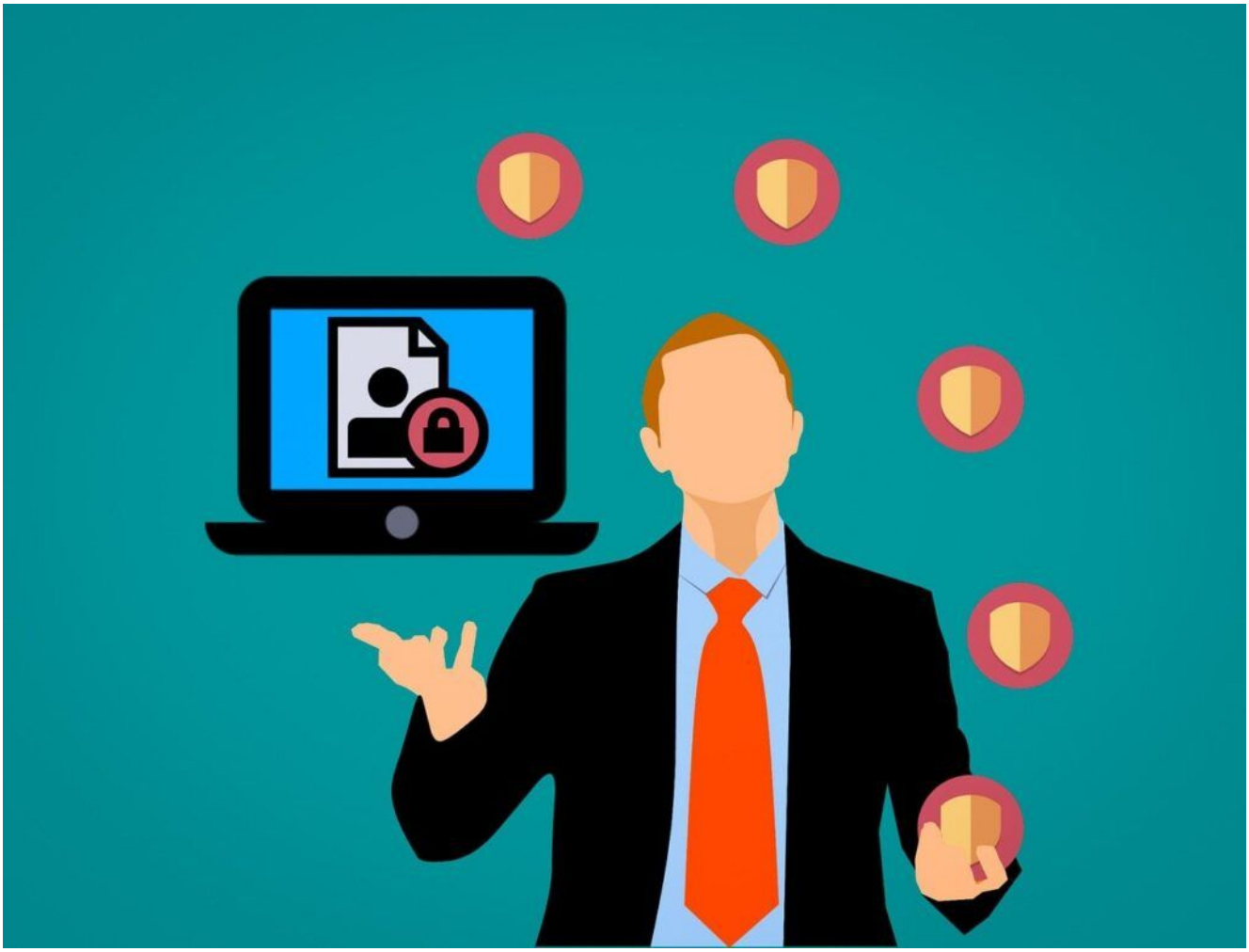
Questo processo di adeguamento è essenziale per garantire la conformità alle leggi sulla privacy e per proteggere i dati personali nell'ambito delle attività aziendali. Seguire queste fasi consentirà alle imprese di gestire correttamente la

privacy e di evitare possibili sanzioni derivanti da violazioni delle normative vigenti.

Analisi e individuazione delle attività di trattamento dei dati

Nel processo di adeguamento alla normativa sulla privacy, ogni azienda deve inizialmente individuare le attività di trattamento dei dati personali effettuate e le tipologie di dati trattati nell'ambito delle proprie operazioni. Questa analisi preliminare è fondamentale per definire una strategia adeguata a garantire la protezione dei dati.

A volte, si può erroneamente credere di non trattare dati personali e di essere esentati dal rispetto delle normative. Tuttavia, anche soggetti come artigiani o piccoli negozi alimentari possono ritrovarsi in possesso di un database di dati personali significativo, ad esempio se conservano elenchi di anagrafiche di clienti o fornitori o se hanno dipendenti.



Una volta identificate le attività di trattamento e i dati personali trattati, è necessario analizzarli con semplici domande:

– *Come raccolgo queste informazioni/dati?*

– *Per quale motivo tratto queste informazioni/dati (finalità del trattamento)?*

– *Sono legittimato a trattarle?*

– *Come le conservo?*

– *Per quanto tempo?*

Per agevolare questa analisi, si consiglia di effettuare una ricognizione dei moduli di raccolta dati, dei contratti e/o dei documenti informativi già in uso, verificare l’acquisizione dei consensi al trattamento quando necessario, individuare le finalità del trattamento e censire gli archivi

digitali e cartacei.

La legittimazione al trattamento dei dati non richiede il consenso dell'interessato per ogni singola finalità, ad esempio nel caso di trattamento dei dati di un cliente per l'esecuzione di una prestazione richiesta.

Questa fase iniziale consentirà all'azienda di avere una visione completa dell'impatto delle proprie attività in termini di privacy.

Valutazione dei rischi e implementazione delle misure di sicurezza per la privacy aziendale

Dopo aver raccolto le informazioni e delineato un quadro generale delle attività di trattamento dei dati svolte, le aziende devono valutare i rischi ad esse associati e implementare le misure necessarie per mitigare tali rischi e garantire la sicurezza dei dati e delle informazioni trattate.

L'obiettivo di questa operazione è ridurre il rischio di perdita, modifica o accesso non autorizzato alle informazioni personali e non solo, detenute dall'azienda.

Una corretta valutazione dei rischi, seguita dall'applicazione di adeguate misure di sicurezza, consente di:

– Ridurre possibili sanzioni o richieste di risarcimento danni da parte degli interessati in caso di violazione dei dati personali (noto come "Data Breach").

– Proteggere il patrimonio informativo dell'azienda, che riveste sempre maggiore importanza nella sua vita operativa.

È importante ricordare che, ai fini della tutela effettiva dei dati personali, il Regolamento Europeo ha introdotto il

principio di “privacy by design” e il principio di “accountability”. Di conseguenza, sono richieste misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio.

La valutazione dei rischi deve considerare gli effetti negativi che una violazione dei dati potrebbe avere sulle libertà e i diritti degli interessati. Il titolare del trattamento può decidere autonomamente se avviare il trattamento o effettuare un’ulteriore analisi più specifica (nota come “Valutazione di Impatto o DPIA”), che potrebbe richiedere la consultazione dell’Autorità Garante per ottenere indicazioni su come gestire il rischio residuo.

Se non è possibile identificare misure di sicurezza “adeguate” in modo generale, è comunque possibile individuare buone pratiche da applicare in ogni azienda, come assicurare un elevato livello di sicurezza informatica. In Italia, infatti, gli attacchi informatici miranti al furto di dati aziendali sono in costante aumento. Termini come ransomware, phishing e data breach sono ormai ben noti a tutti.

L’uso di un buon antivirus, un firewall, password complesse e regolarmente cambiate, nonché una gestione efficace delle reti informatiche, rappresentano ancora le principali difese per proteggere i dati archiviati digitalmente.

È altresì fondamentale garantire la capacità di ripristinare tempestivamente la disponibilità e l’accesso ai dati personali in caso di incidenti fisici o tecnici. Ad esempio, se un vecchio computer smettesse improvvisamente di funzionare o venisse hackerato, la perdita anche temporanea dei dati rappresenterebbe un grave problema per l’azienda. In questi casi, un backup regolare dei dati su dispositivi sicuri rappresenta una soluzione semplice e accessibile per salvaguardare le informazioni.

Tutte queste misure di sicurezza devono essere accompagnate da una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative adottate.

Misure di sicurezza e privacy aziendale: guida sintetica per le imprese

Inoltre, è importante rafforzare le misure di sicurezza organizzative al fine di consentire una gestione ordinata e consapevole delle attività, semplificando il lavoro e coinvolgendo tutti i soggetti interessati. Ciò può includere la definizione di procedure specifiche per affrontare eventuali violazioni delle informazioni, gestire le richieste degli interessati e regolare l’uso degli strumenti informatici. Questo passaggio è fondamentale per garantire un’adeguata impostazione del trattamento dei dati per l’intera durata del processo.

Infine, tra le misure organizzative, la formazione del personale riveste un ruolo essenziale. Anche le migliori misure di sicurezza saranno inefficaci se coloro che operano all’interno dell’azienda (e che trattano concretamente i dati personali) non sono stati adeguatamente formati e istruiti.

Investire nella formazione e nell’aggiornamento del personale sulle norme di sicurezza e privacy è fondamentale per creare una cultura aziendale che metta al centro la protezione dei dati.

La valutazione dei rischi e l’implementazione di misure di sicurezza adeguate sono passaggi cruciali per garantire la protezione dei dati personali all’interno di un’azienda. È importante considerare le specificità del contesto aziendale e adattare le misure di sicurezza in base al livello di rischio identificato. Inoltre, è fondamentale mantenere una costante attenzione e monitoraggio per adattare e migliorare le misure di sicurezza nel tempo, tenendo conto delle nuove minacce e delle evoluzioni normative nel campo della privacy.

La figura del Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

La figura del Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO) ha un ruolo chiave assegnato dal legislatore, con compiti e poteri specifici, che includono la sensibilizzazione e la formazione del personale, la consulenza al Titolare e la vigilanza sul rispetto del GDPR.

Secondo l’articolo 37 del GDPR, la designazione del RPD è obbligatoria solo in determinate circostanze:

a) il trattamento deve essere effettuato da un’autorità pubblica o da un organismo pubblico, ad eccezione delle autorità giurisdizionali quando agiscono nel loro ambito giurisdizionale;

b) le attività principali del Titolare del trattamento o del Responsabile del trattamento devono coinvolgere trattamenti che, per loro natura, ambito o finalità, richiedono il monitoraggio regolare e sistematico su larga scala degli interessati;

c) le attività principali del Titolare del trattamento o del Responsabile del trattamento devono coinvolgere il trattamento su larga scala di categorie particolari di dati personali di cui all’articolo 9 o di dati relativi a condanne penali e reati di cui all’articolo 10 del GDPR.

Questi elementi di solito emergono durante la prima analisi che l’azienda deve effettuare. Sarà quindi compito del Titolare valutare la necessità o l’opportunità di nominare un Responsabile della Protezione dei dati.

Predisposizione dell’informativa privacy per gli interessati

Dopo aver identificato i dati personali trattati e aver stabilito una corretta politica di raccolta e conservazione, l’azienda deve garantire agli interessati la possibilità di esercitare tutti i diritti previsti dal GDPR.

Il primo di questi diritti è senza dubbio il diritto dell’interessato ad essere informato.

L’azienda è tenuta a fornire all’interessato una serie di informazioni, tra cui:

– L’identità e i dati di contatto del responsabile del trattamento dei dati (il cosiddetto titolare del trattamento).

– I dati di contatto del responsabile della protezione dei dati, se presente.

– Le finalità del trattamento e la base giuridica corrispondente.

– Eventuali destinatari o categorie di destinatari a cui i dati personali potrebbero essere comunicati.

– Il periodo di conservazione dei dati personali o, se non è possibile specificarlo, i criteri utilizzati per determinare tale periodo.

– I diritti dell'interessato e i canali per esercitarli, nonché il diritto di presentare reclamo all'Autorità Garante.

– L'eventuale obbligatorietà di fornire i dati personali e le possibili conseguenze del mancato conferimento.

Privacy aziendale: guida sintetica per le imprese

Hanno parlato di noi

CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi

Libero Quotidiano.it

fanpage.it

PANORAMA

TGCOM24

TG5

Rai News 24

Rai 1

Rai 2

Rai 3

Rai Radio 1

CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

Contattaci

- Orari

Lunedì – Venerdì: 9.00 – 13.00 / 14.30 – 19.00

Lunedì – Venerdì:
9.00 – 13.00 / 14.30 – 19.00

- Email

info@alassistenzalegale.it

- Telefono

+39 3453338510

- WhatsApp

+39 3453338510

Chiamaci
Contattaci

☐ Ho letto e accetto i termini dell'Informativa sulla Privacy
Invia