GHIRO srl Servizi all'impresa
Via Crispi 19 – 21100 Varese –
tel: 0332 804723 e-mail: info@ghirosrl.it - Pec ghiro.srl@legalmail.it
C.F., p.IVA e registro imprese: 03274410129 - - Cap.soc. 30.000€ i.v.

CIRCOLARE PRIVACY – DICEMBRE 2024

➔ Data Breach: Importanza della Notifica Dettagliata al Garante

Attenzione alla Compliance (Conformità) con il GDPR È fondamentale rispettare l'obbligo di notificare dettagliatamente ogni violazione dei dati al Garante della Privacy, come richiesto dall'art. 33 del GDPR (Regolamento UE 2016/679). Non adempiere in modo esaustivo a questo obbligo può comportare pesanti sanzioni. Un recente caso ha visto una sanzione di 900 mila euro per una società che, a seguito di un attacco ransomware, ha visto pubblicati sul dark web i dati personali di circa 25 mila persone. L'azienda aveva notificato l'evento al Garante con informazioni insufficienti, nonostante precedenti avvisi delle autorità per aggiornare i sistemi di sicurezza.

Il Garante ha ribadito che **la notifica deve contenere tutti i dettagli pertinenti dell'incidente, i server coinvolti e le vulnerabilità sfruttate**. Notifiche incomplete rischiano di compromettere il processo di verifica e aumentare le sanzioni.

Fonte: *Italia Oggi, articolo di Antonio Ciccia Messina*

Autovalutazione per la Gestione dei Data Breach:

- La mia azienda è pronta a gestire una notifica dettagliata di data breach al Garante?
- Quali procedure interne sono attivate per garantire una comunicazione completa e tempestiva, evitando notifiche generiche o incomplete?
- Abbiamo aggiornato periodicamente i sistemi informatici e implementato misure di sicurezza contro i rischi segnalati?

➔ Nomina degli Incaricati Privacy: Rilevanza della Firma di Accettazione

Conseguenze per il Mancato Accoglimento della Nomina Privacy Con l'ordinanza n. 504/2024 del Tribunale di Udine, è stato stabilito che un dipendente che rifiuti di firmare la nomina come incaricato privacy può essere sospeso dal lavoro e dalla retribuzione. Questo pronunciamento ha messo in evidenza come il rifiuto di accettare la nomina comprometta la capacità del dipendente di trattare i dati personali in maniera legittima, potenzialmente impedendogli di svolgere le proprie mansioni.

La designazione come incaricato è fondamentale, poiché consente al dipendente di operare con consapevolezza, rispettando la normativa e le policy aziendali.

Autovalutazione per la Nomina degli Incaricati Privacy:

- Qual è la procedura interna per nominare gli incaricati al trattamento dei dati personali?
- Come gestiamo un rifiuto alla nomina?
- Quali programmi di formazione sono attuati per istruire adeguatamente gli incaricati sulle responsabilità derivanti dal GDPR?

GHIRO srl Servizi all'impresa
Via Crispi 19 – 21100 Varese –
tel: 0332 804723 e-mail: info@ghirosrl.it - Pec ghiro.srl@legalmail.it
C.F., p.IVA e registro imprese: 03274410129 - - Cap.soc. 30.000€ i.v.

CIRCOLARE PRIVACY – DICEMBRE 2024

➔ Responsabili del trattamento di dati: la scelta deve ricadere solo su soggetti che garantiscano misure di sicurezza adeguate al rispetto del GDPR

L'European Data Protection Board (EDPB) ha emesso il Parere 22/2024, rispondendo all'Autorità danese riguardo agli obblighi dei titolari del trattamento (Titolari) nell'utilizzo di responsabili (Responsabili) e sub-responsabili del trattamento.

Il documento evidenzia che **i Titolari devono assicurarsi** che i propri **fornitori** Responsabili e i loro Sub-responsabili adottino misure di sicurezza adeguate a rispettare il GDPR. Essi devono essere in grado di identificare tutti i fornitori coinvolti nel trattamento, e i Responsabili devono fornire informazioni dettagliate e tempestive sui loro Sub-responsabili per facilitare adempimenti come la gestione dei registri dei trattamenti e la notifica di eventuali data breach.

L'EDPB sottolinea che **i Titolari dovrebbero selezionare solo Responsabili che garantiscano misure tecniche e organizzative idonee** e che eseguano audit periodici sui fornitori. Possono richiedere copie dei contratti con i Sub-responsabili per verificare che rispettino gli stessi obblighi previsti per i Responsabili, sebbene ciò non sia un obbligo ma un diritto.

L'EDPB ricorda anche che i Titolari rimangono responsabili per il trasferimento di dati verso paesi terzi, evidenziando la necessità di documentare valutazioni di impatto e misure di sicurezza. Infine, l'EDPB consiglia di specificare nei contratti con i Responsabili che questi devono seguire solo le istruzioni del Titolare, salvo obblighi legali di trattamento.

Autovalutazione per la gestione dei Fornitori:

- L'azienda è in grado di identificare tutti i responsabili e sub-responsabili coinvolti nel trattamento dei dati personali, con informazioni precise sulla loro identità e ruolo?
- Prima di scegliere un responsabile del trattamento, l'azienda verifica che siano presenti garanzie sufficienti per l'implementazione di misure tecniche e organizzative conformi al GDPR?
- L'azienda svolge regolari audit o chiede evidenze documentali ai responsabili per monitorare le loro misure di sicurezza e compliance, anche in relazione ai sub-responsabili?
- I contratti con i responsabili del trattamento includono chiare istruzioni documentate che precisano che i dati devono essere trattati solo su direttiva del titolare, salvo disposizioni di legge?

Telemarketing: il Garante Privacy sanziona Sky Italia

Sky Italia è stata multata per 840 000 euro per **violazioni legate al trattamento dei dati personali durante campagne di telemarketing e invio di SMS promozionali**. Le principali infrazioni includono:

- Mancato controllo del Registro Pubblico delle Opposizioni.
- Utilizzo di consensi non validi o datati, anche antecedenti al GDPR.
- Conservazione dei consensi in file Excel modificabili, privi di garanzie di autenticità.
- Considerazione di consensi obbligatori o impliciti come validi.
- Il Garante ha imposto misure correttive per garantire la liceità dei trattamenti futuri e vietato l'uso di dati personali della piattaforma NOW senza esplicito consenso.

Fonte: *Ufficio stampa Garante Privacy*

Via Crispi 19 – 21100 Varese –
tel: 0332 804723 e-mail: info@ghirosrl.it - Pec ghiro.srl@legalmail.it
C.F., p.IVA e registro imprese: 03274410129 - - Cap.soc. 30.000€ i.v.

CIRCOLARE PRIVACY – DICEMBRE 2024

Autovalutazione per le attività di marketing:

- L'informativa sulla privacy fornita agli utenti specifica chiaramente le finalità del trattamento dei dati (es. invio di newsletter)?
- Gli utenti forniscono il consenso esplicito per ricevere newsletter e altre comunicazioni promozionali?
- Come vengono raccolti e registrati i consensi degli utenti? Il sistema permette di documentare chiaramente le modalità e i tempi del consenso?
- I fornitori esterni (es. piattaforme per la gestione di newsletter) sono stati valutati per garantire la conformità al GDPR?
- È stata definita una procedura per gestire eventuali reclami da parte degli utenti in merito a invii non autorizzati o errori di gestione?

Grazie dell'attenzione

Per ogni informazione scrivere a katia.langini@ghirosrl.it