Lloyd's Register

Improving performance, reducing risk

Il Regolamento generale sulla protezione dei dati (GDPR)

Che cos'è il GDPR?

Il Regolamento generale sulla protezione dei dati (GDPR) offre una maggiore tutela alle persone fisiche e rende le aziende più responsabili nell'uso dei dati personali. Grazie a questo nuovo Regolamento, la protezione dei dati assume una posizione di prima linea tra i processi aziendali, con un impatto significativo sulla gestione delle informazioni personali relative sia ai clienti che ai dipendenti.

Il Parlamento Europeo, nell'aprile 2016, ha approvato il Regolamento Generale sulla Protezione dei Dati (GDPR) [Regolamento (UE) 2016/679], che entrerà in vigore a partire dal 25 maggio 2018.
Il Regolamento andrà a rafforzare il livello di tutela dei dati per tutte le persone fisiche all'interno dell'UE indipendentemente da dove sono custoditi i dati. Messo a punto sulla base della legislazione esistente, il nuovo Regolamento mira a migliorare la coerenza legislativa e le tutele già in vigore.

A chi si applica?

L'articolo 3 del GDPR ne definisce il campo di applicazione territoriale, che riguarda:

- Il trattamento dei dati personali nel contesto delle attività delle organizzazioni / aziende dell'Unione Europea, indipendentemente dal fatto che il trattamento dei dati sia effettuato o meno all'interno dell'Unione.
- Il trattamento dei dati personali di interessati (es. persone in vita) che si trovano nell'Unione da parte di un responsabile del trattamento o incaricato del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano l'offerta di beni o servizi ai suddetti interessati nell'Unione, o il controllo del loro comportamento all'interno l'Unione.
- Il trattamento di dati personali da parte di organizzazioni /aziende non stabilite nell'Unione, ma in un luogo soggetto al diritto nazionale mediante misure tecniche e organizzative adeguate.

I sei principi del GDPR

L'articolo 5 stabilisce che i dati personali devono essere:

1. Trattati in modo lecito, equo e trasparente nei confronti dell'interessato.
2. Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità; un ulteriore trattamento dei dati personali per finalità di archiviazione non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali.
3. Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
4. Esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti.
5. Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quanto sia necessario; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento a tutela dei diritti e delle libertà dell'interessato.
6. Trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate.

Chi è responsabile della protezione dei dati?

Il (Data Protection Officer - DPO) rappresenta all'interno dell'organizzazione / azienda il volto indipendente della protezione dati. Tutte le organizzazioni / aziende devono provvedere a dotarsi di competenze e risorse sufficienti a soddisfare i propri requisiti di GDPR e, in alcuni casi, il Regolamento prevede anche la necessità di nominare un DPO.

I compiti minimi di un DPO vengono specificati all'articolo 39 del Regolamento:

- Informare e consigliare l'organizzazione/ azienda e i suoi dipendenti riguardo agli obblighi vigenti in materia di protezione dei dati.
- Sorvegliare l'osservanza del Regolamento, e delle altre disposizioni relative alla protezione dei dati, compresa la sensibilizzazione e formazione dei dipendenti, fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati e provvedere alla conduzione di audit interni.
- Fungere da punto di contatto per le autorità di controllo sulle questioni relative al trattamento dei dati personali e al rispetto delle norme vigenti in materia.
- Valutare i rischi inerenti al trattamento dei dati.

Come Lloyd's Register vi può essere di aiuto?

WORKSHOP RESPONSABILE PROTEZIONE DATI

Se state per assumere il ruolo di DPO, il workshop di due giorni di LRQA vi aiuterà a conoscere dettagliatamente ruolo e responsabilità previsti per un DPO dal GDPR.
Il nostro workshop vi offrirà gli strumenti pratici per realizzare sistemi efficaci e coinvolgere la vostra azienda per il pieno rispetto dei requisiti del nuovo regolamento.
Al corso vi verranno fornite informazioni su:

- il ruolo del DPO e su come attuare e gestire, in qualità di RPD, un sistema che sia conforme a quanto previsto dal GDPR.
- come impostare un programma di protezione dati conforme al Regolamento, che sia sostenibile, efficace e basato sul rischio.
- come realizzare le relative politiche, procedure e materiale informativo sull'argomento.
- come promuovere il coinvolgimento a tutti i livelli aziendali e come comunicare con i vari stakeholder.
- il ruolo del DPO in situazioni di crisi.

WORKSHOP VALUTAZIONE IMPATTO PROTEZIONE DATI (DPIA)

Possiamo offrire una formazione relativa alla DPIA con indicazioni pratiche su come condurne una specifica per la vostra azienda.
Se siete responsabili della realizzazione di una DPIA, il nostro workshop di un giorno presso la vostra azienda vi offrirà una guida pratica alla realizzazione di una Valutazione d'Impatto sulla Protezione Dati (DPIA), che comprende:

- Che cos'è una DPIA e quando la si deve fare.
- Raccomandazioni e orientamenti dei vostri enti di normazione nazionali.
- Le fasi di una DPIA e cosa si deve fare in pratica.
- Il rapporto tra la conduzione di una DPIA e altri interventi di gestione del rischio e di project management, come ad esempio altri audit per la valutazione dei rischi o protezione dei dati.
- Quali aspetti legali e di conformità alle norme vanno presi in considerazione nella vostra azienda.

ISO: 22301:2012

ISO 22301:2012, la norma internazionale per la continuità del business, identifica le buone pratiche nella costituzione di un sistema di gestione che minimizzi i rischi degli impatti derivanti da un'interruzione nella fornitura di servizi. Come la maggior parte degli standard internazionali per i sistemi di gestione, si basa sul ciclo di Deming, ovvero: Pianificare - Fare - Verificare - Agire.

Un sistema di gestione della continuità del business non solo aiuta le aziende a creare le strutture per identificare potenziali minacce e valutare l'impatto causato da incidenti e come affrontarli, ma offre anche un contesto per la gestione organizzativa attraverso un processo di predisposizione di strategie e metodi atti a ridurre l'impatto del singolo incidente, sviluppando le capacità per rispondere efficacemente al suo eventuale verificarsi. Alla luce di ciò, un sistema di gestione offre un meccanismo perfetto per la gestione delle eventuali violazioni nel campo della protezione dati.

5 fasi di attuazione Piano del Regolamento Generale sulla Protezione dei Dati (GDPR)

1. Sensibilizzazione
Aumentare la conoscenza del GDPR nella vs. azienda.
Da una panoramica generale alla conoscenza necessaria al singolo ruolo per garantire il rispetto del Regolamento.

2. Mappatura dati
Identificare situazione attuale.
Qual è la situazione della vs. azienda? Identificazione dei rischi e degli interventi necessari, attraverso una mappatura dei dati, il riesame delle politiche, dei processi e delle pratiche e un'approfondita *gap analysis*.

3. Messa a punto di un piano d'intervento
Stesura piano d'intervento GDPR.
Coinvolgimento di tutti coloro che all'interno dell'azienda si impegneranno ad attuare il piano assumendosene la responsabilità.

4. Implementazione piano
Agire e attuare quanto pianificato.
Definizione delle tempistiche di attuazione e gestione dell'implementazione secondo gli obiettivi previsti dal piano d'intervento.

5. Gestire e migliorare il vostro sistema
Dimostrazione conformità e impegno.
Esame dei risultati ottenuti a oggi rispetto ai *gap* identificati nella fase 2.
Riesame del sistema con controlli continui per garantirne la costante efficacia.

Lloyd's Register
Via Cadorna, 69
20090 Vimodrone (MI)
Italy

Tel. : +39 02 365 7541
Email : certificazione@lr.org

Sito web : www.lrqa.it

www.lrqa.it