

Perché assicurarsi nell'era del GDPR

Bologna, 09/10/2019

UNIONCAMERE EMILIA ROMAGNA

Chi siamo

Assicoop Bologna Metropolitana SpA è l'Agenzia che principalmente rappresenta UnipolSai Assicurazioni nella città di Bologna, (compreso il territorio Imola) - dove è leader di mercato.

Dispone di 40 punti vendita, dove lavorano oltre 250 persone, e si avvale di una Rete di Consulenti specializzati nei diversi segmenti di mercato: *aziende, professionisti, famiglie.*

Assicoop Bologna Metropolitana raccoglie oltre 151 milioni di euro di premi assicurativi totali e conta , tra i suoi 72.500 Clienti, circa 8.000 Aziende, che comprendono alcune fra le maggiori Imprese bolognesi e diversi Enti Locali.

Come lavoriamo

Assicoop Bologna Metropolitana SpA, è organizzata per rispondere in modo puntuale e qualificato alle Imprese di ogni dimensione e complessità

- Per le Grandi Imprese:
attraverso gli **Account dell'Area Imprese e Large Corporate**, per una gestione altamente specializzata dei rischi. Partendo da un'analisi basata sulla metodica del Risk Management, si definiscono pacchetti assicurativi specifici per le aree di rischio individuate
- Per le PMI, gli Artigiani e i Professionisti:
attraverso i **Consulenti** dedicati, per la messa a punto di piani assicurativi tarati sulle caratteristiche e le esigenze dei Clienti.

Perché assicurarsi nell'era del GDPR? Esigenze assicurative

Quali sono i **principali rischi** in ambito privacy?

- Richieste di risarcimento da parte degli Interessati al trattamento a seguito di diffusione / perdita / danneggiamento di dati personali
- Sanzioni inflitte alle imprese presso cui il DPO ha prestato la propria attività di consulenza privacy

Quali sono le **figure esposte a richieste di risarcimento** nell'ambito della nuova disciplina privacy?

- Titolare del trattamento Dati
- Responsabile del trattamento dei Dati
- Data Protection Officer

Proposta assicurativa di UnipolSai

Per le imprese



Copertura per la responsabilità civile derivante dall'**errato trattamento dei dati personali rivolta alle imprese**

Copertura Cyber Risks per la responsabilità civile derivante dall'**errato trattamento dei dati personali azienda**

Polizza di Responsabilità Civile degli amministratori con estensione **trattamento dei dati personali**

Per i professionisti



Polizza di responsabilità civile per il professionista/studio associato che svolge **esclusivamente e/o in maniera accessoria l'attività di DPO**

Garanzia RC errato trattamento dati per le Imprese



UnipolSai propone in garanzia base una copertura per la **responsabilità civile derivante dall'errato trattamento dei dati personali** attraverso un'estensione di garanzia su polizza RCT Azienda.

Estensione su polizza RC Azienda

La garanzia opera per la responsabilità civile derivante all'Assicurato ai sensi della vigente Normativa per la protezione dei Dati personali, a seguito di Perdite patrimoniali cagionate a terzi interessati, compresi i clienti, in conseguenza di trattamento dei loro Dati personali (raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione) non conforme alla normativa, purché conseguenti a fatti involontari e non derivanti da comportamento illecito continuativo.

La presente garanzia vale per la responsabilità derivante all'Assicurato:

- a) per le funzioni svolte in qualità di Titolare del trattamento Dati;
- b) per l'attività del Responsabile del trattamento dei Dati, nominato dall'Assicurato e operante per conto dello stesso;
- c) per l'eventuale attività svolta dal Responsabile della protezione dati (RPD) o Data Protection Officer (DPO), interno, nominato dall'Assicurato e operante per conto dello stesso.

Adeguamento agli standard di protezione GDPR

Primi passi per la messa in sicurezza dei dati, prima di trasferire il rischio alla Compagnia di Assicurazione:

Lo Standard è finalizzato al rilascio di una dichiarazione di conformità con le procedure connesse ai criteri definiti dal Regolamento europeo sulla Protezione dei Dati (GDPR)

L'applicazione dello Standard , concepito per qualunque tipo di azienda o organizzazione, concerne determinati aspetti relativi alla protezione dei dati personali delle attività, dei prodotti e dei servizi dell'azienda/organizzazione ed è finalizzato a:

- Fornire supporto nel quadro del rispetto degli obblighi definiti dal Regolamento (UE) 2016/679
- Identificare, proteggere e trattare i dati personali
- Monitorare i punti di controllo e i dati trattati - Comunicare con autorità e parti interessate

In che modo la certificazione può aiutarvi?

Al fine di valutare l'efficacia delle procedure e dei processi implementati per garantire la sicurezza delle attività di trattamento, Valutazioni delle Procedure di Controllo, Analisi degli scostamenti

Estensione in ambito polizza Rc Amministratori

Assicurato:

il soggetto cui spettano i diritti derivanti dal contratto ed in particolare i componenti il Consiglio di Gestione, i componenti il Consiglio di Sorveglianza, i componenti il Consiglio di Amministrazione, il/i Direttore/i Generale *esclusivamente di nomina assembleare o statutaria*, i componenti il Collegio Sindacale, *per l'espletamento delle cariche indicate nella Proposta Questionario*, i componenti dell'Organo collegiale di Vigilanza (come disciplinato dal D.lgs. 231/2001), i dirigenti della Contraente *nell'espletamento delle proprie funzioni di direzione, organizzazione e controllo per conto della stessa*, **il dipendente/dirigente designato quale responsabile del trattamento dei dati personali (D. lgs. n.196/2003 – GDPR 25-05-2018) qualora l'atto dannoso a lui riferibile riguardi l'esercizio di funzioni manageriali o di supervisione.**

• CYBER RISK: definizioni

Il **Cyber Risks** inteso come rischio operativo relativo alle **informazioni/dati** e agli **asset tecnologici** che comporta conseguenze in ordine alla **riservatezza**, **disponibilità** o **integrità** delle informazioni o dei sistemi informativi.

Information Technology Asset

Il complesso delle informazioni, dei software o hardware di proprietà di un'organizzazione che vengono adoperati nel corso delle attività di business

Impianto o sistema di elaborazione dati

la totalità delle apparecchiature elettroniche (unità centrali, periferiche, apparecchiature di servizio), elettricamente coordinate, necessaria per l'espletamento delle funzioni di elaborazione

Dati

Insieme di informazioni logicamente strutturate, elaborabili a mezzo di programmi

Sistemi informativi

quel complesso di elementi che rileva in modo sistematico e organizzato i fenomeni economici di interesse dell'azienda, nell'intento di rappresentarli in modo organico, utilizzando la tecnologia più appropriata ed applicando logiche e metodi suggeriti, per le diverse classi dei fenomeni aziendali, dalle discipline di economia aziendale

Statistiche: alcuni numeri sul cyber risk

Ogni minuto 232 computer sono infettati da malware

In Europa il *consumer cybercrime*, ovvero la criminalità informatica a danno dei consumatori, ha un costo di 16 miliardi di USD

La violazione della sicurezza di una rete informatica comporta un costo medio di oltre 5 milioni di USD

La violazione della sicurezza di una rete informatica ha un costo medio per record pari a 150 USD

Nuovi e sofisticati attacchi sono costantemente messi a punto da parte di soggetti molto diversi: organizzazioni criminali, hacker, dipendenti di aziende, *hactivist* (attivisti digitali),

- **CYBER RISK: segue**

Rischi per le aziende – IoT e SCADA

Società che sia avvale di **Strumenti IoT** o di **sistemi SCADA**

IoT

acronimo dell'inglese Internet of Things, è un neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti.

SCADA

l'acronimo SCADA, dall'inglese "Supervisory Control And Data Acquisition", cioè "controllo di supervisione e acquisizione dati" indica un sistema informatico utilizzato per il monitoraggio e il controllo elettronico di sistemi fisici, quali impianti industriali e infrastrutture distribuite geograficamente sul territorio.

in caso di Attacco Cyber potrebbe subire una **riduzione o interruzione della produzione**, incidenti che provocano infortuni o decessi del personale , **danneggiamenti alle infrastrutture** e danni ambientali

• CYBER RISK: policy

Gli **impatti negativi** che potrebbero derivare dal verificarsi di un evento cyber sono **trasferibili** tramite la sottoscrizione di **una polizza CYBER RISK** a copertura del:

❖ **Danno all'organizzazione (First party damage):**

- **Danni materiali (diretti):** la distruzione o deterioramento di cose;
- **Perdite patrimoniali:** danno indiretto, che costituisce un pregiudizio economico non immediatamente conseguente a danni corporali o danni materiali.
- **Costi per la gestione della crisi**

❖ **Danno cagionato a terzi (Third party damage):**

- **Danni materiali;**
- **Danni alla persona;**
- **Perdite patrimoniali.**

Polizza di responsabilità civile del DPO

La Garanzia Perdite patrimoniali comprende le seguenti fattispecie



Sanzioni fiscali, amministrative e/o pecuniarie in genere, multe e/o ammende **inflitte ai soggetti presso i quali l'Assicurato svolge o ha svolto la propria attività** descritta in polizza



Danneggiamenti, distruzione, perdita, sottrazione di documenti, atti, titoli non al portatore, escluso comunque il furto, rapina ed incendio



Interruzione e/o sospensione (totale o parziale), mancato o ritardato inizio di attività in genere esercitate da terzi a seguito di errori commessi dall'assicurato nell'espletamento dell'attività descritta in polizza



Mancata, errata, ritardata e/o incompleta predisposizione di pratiche amministrative inerenti l'attività descritta in polizza



Lucro cessante per mancato guadagno, in quanto conseguenza immediata **dell'inadempimento o dell'illecito commesso dall'assicurato nello svolgimento della propria attività professionale**