MARSH

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

LEADERSHIP, KNOWLDGE, SOLUTIONS…WORDLWIDE.

MARSH & McLENNAN COMPANIES

QUESTIONARIO ASSICURATIVO POLIZZA CYBER

Nota: la polizza richiesta attraverso il presente questionario è una polizza prestata nella forma " claims made" ed è soggetta alle relative condizioni. Questa polizza è valida solo in seguito alla richiesta di risarcimento da parte degli assicurati, segnalata per iscritto agli assicuratori entro il termine della polizza o dell'eventuale periodo di osservazione, se applicabile. I costi sostenuti come rimborso spese possono ridurre ed esaurire il limite di responsabilità e sono soggetti a franchigia.

Si prega di leggere e compilare attentamente il seguente questionario.

Sezione 1. Informazioni generali sulla Proponente

1.1 Proponente

Ragione Sociale:	Sogei S.p.A.
Indirizzo:	Via Mario Carucci 99 - 00143 Roma
Sede legale:	Via Mario Carucci 99 - 00143 Roma
Telefono:	06 50251
Indirizzo Web:	www.sogei.it

1.2 La Proponente è continuamente in attività dal: 1976

1.3 Descrizione dell'attività svolta dalla proponente: prestazione di servizi strumentali all'esercizio delle funzioni pubbliche attribuite al Ministero dell'Economia e delle Finanze e alle Agenzie !scali e, in particolare, ogni attività !nalizzata alla realizzazione, allo sviluppo, alla manutenzione e alla conduzione tecnica del Sistema informativo della !scalità (SIF) per l'Amministrazione !nanziaria, la realizzazione delle attività informatiche riservate allo Stato ai sensi del decreto legislativo n. 414 del 1997, e successivi provvedimenti di attuazione, ivi comprese le attività di supporto, assistenza e consulenza collegate a tali attività, nonché le attività di sviluppo e gestione dei sistemi informatici e ogni altra attività di carattere informatico in aree di competenza del Ministero dell'Economia e delle Finanze.

1.4 Numero di Dipendenti: 2124

1.5 Si prega di allegare copia dell'ultimo bilancio

1.6 Fatturato della Proponente:

	Annualità		
	Precedente	Corrente	Prossima
Totale Fatturato Cosolidato	€ 520.363.899	€ 539.856.574	€ Fare clic qui per immettere testo.

Ripartizione geografica del fatturato della Proponente (%)			
Unione Europea	€ 100 %	€ 100%	€ Fare clic qui per immettere testo.
USA/CANADA	€ Fare clic qui per immettere testo.	€ Fare clic qui per immettere testo.	€ Fare clic qui per immettere testo.
Resto del Mondo	€ Fare clic qui per immettere testo.	€ Fare clic qui per immettere testo.	€ Fare clic qui per immettere testo.

1.7 Si prevedono cambiamenti significativi nella natura o nella dimensione del business della proponente nei prossimi dodici (12) mesi? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

1.8 Vi sono stati cambiamenti di questo genere negli ultimi 12 mesi (12) mesi? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

1.9 Negli ultimi dodici (12) mesi, la Proponente ha completato o concordato una fusione, acquisizione o consolidamento? (sia che queste operazioni siano state portate a termine o meno) SI☐ NO☒

1.10 La Proponente ha intenzione di portare a termine operazioni di questo tipo nei prossimi dodici (12) mesi? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

Sezione 2. Carte di Pagamento

2.1 La proponente è dotata di un e-commerce attraverso il quale effettua attività di vendita? SI☐ NO☒

Se si:

2.1.1 Indicare la percentuale di fatturato derivante da vendite effettuate tramite l'e-commerce:

2.2 La proponente accetta pagamenti con carta di credito per beni o servizi? SI☐ NO☒

Se si:

2.2.1 Indicare la percentuale dei ricavi da transazioni con carta di credito negli ultimi dodici (12) mesi: Fare clic qui per immettere testo.

2.3 La proponente(se soggetta) è conforme alle vigenti norme di sicurezza emesse dalle istituzioni finanziarie con le quali è convenzionata (Payment Card industry Data Security Standards PCI DSS)?

NON SOGGETTA ☐
CONFORME ☒
NON CONFORME ☐

Se non conforme:

2.3.1 Si prega di descrivere lo stato attuale di qualsiasi opera di adeguamento e la relativa data di completamento prevista: Fare clic qui per immettere testo.

2.4 La proponente processa pagamenti per conto di altri, comprese transazioni e-commerce? SI☐ NO☒

Se si:

2.4.1 Si prega di fornire il numero di clienti per cui vengono gestiti i pagamenti e una stima del numero di transazioni per cliente: Fare clic qui per immettere testo.

Sezione 3. Gestione delle esposizioni della privacy

3.1 La Proponente è in possesso di una policy sulla privacy a livello aziendale? SI☒ NO☐

3.2 Negli ultimi due anni, la Proponente ha effettuato verifiche interne o esterne relative alla privacy o ha ottenuto un certificato di adeguatezza dei sistemi adottati per la privacy? SI☒ NO☐

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

3.3 La Proponente limita all'uso lavorativo l'accesso dei dipendenti alle informazioni personali? SI☒ NO☐

3.4 Indicare quale tipo di dati, e in che quantità, sono registrati nel database: Si veda risposta alla domanada n. 85

Tipologia	Barrare se registrate	Numero di record
Dati su carte di credito/debito	☐	Fare clic qui per immettere testo.
Dati sensibili (Informazioni sanitarie)	☐	Fare clic qui per immettere testo.
Dati personali	☐	Fare clic qui per immettere testo.
Proprietà Intellettuali del cliente	☐	Fare clic qui per immettere testo.
Altro *(specificare sotto)*	☐	Fare clic qui per immettere testo.

Sezione 4. Controlli dei sistemi informatici

4.1 La proponente pubblica e distribuisce ai propri dipendenti le policy sui sistemi informativi? SI☒ NO☐

4.2 La Proponente esige un feedback positivo da ciascun dipendente sulla comprensione ed accettazione delle policy di cui sopra? SI☒ NO☐

4.3 La Proponente organizza corsi di formazione ai dipendenti che fanno uso dei sistemi informativi sulle problematiche di sicurezza e le procedure per l'utilizzo dei sistemi informatici? SI☒ NO☐

Se si, si prega di indicare la frequenza di tali corsi: Fare clic qui per immettere testo.

4.4 La Proponente dispone di un:

Piano di disaster recovery	SI☒	NO☐
Piano di business continuity	SI☐	NO☒
Piano di risposta alle intrusioni di rete e infezioni da virus	SI☒	NO☐

Se si dispone di uno o più dei sopra-citati documenti, *si prega di allegarne copia.*

4.5 La Proponente dispone di un programma che metta alla prova e testi periodicamente i controlli di sicurezza? SI☒ NO☐

Se si, si prega di fornire informazioni su tali test: In caso di test con esito negativo, si procede con azioni correttive.

4.6 La Proponente sospende tutti gli accessi si computer e agli account quando un dipendente lascia l'azienda?

SI☒ NO☐

4.7 Selezionare quali tra i seguenti strumenti sono implementati nelle infrastrutture di rete della proponente :

Controlli di accesso alla rete	☒
Anti virus	☒
Firewall	☒
Rilevatori di intrusione	☒

4.8 Indicare se la Proponente ha svolto un security, un penetration test oppure una vulnerability assessment audit negli ultimi 24 mesi SI☒ NO☐

Si prega di fornire maggiori dettagli in merito ai risultati dei suddetti test: Fare clic qui per immettere testo.

4.9 Indicare se la Proponente incoraggi l'uso di password complesse ed effettui verifiche periodiche sulle modalità di accesso degli utilizzatori SI☒ NO☐

4.10 Indicare se i laptop siano o meno protetti da firewall personali e/o i laptop possano connettersi solo tramite la rete aziendale SI☒ NO☐

4.11 La Proponente esegue il backup quotidiano di tutti i dati rilevanti/sensibili? SI☒ NO☐

Se no, si prega di indicare le eccezioni: Fare clic qui per immettere testo.

4.12 La Proponente dispone di un backup completo di tutti i file in un luogo sicuro diverso dalla sede centrale delle operazioni? SI☒ NO☐

Se no, descrivere le procedure utilizzate dalla Proponente, se presenti, per archiviare o proteggere le copie dei dati importanti/sensibili fuori sede: Fare clic qui per immettere testo.

4.13 La Proponente possiede e applica una regolamentazione in materia di crittografia della comunicazione interna ed esterna? SI☒ NO☐

4.13.1 I computer e i dispositivi portatili (come ad esempio le chiavi USB) sono protetti da crittografia? SI☐ NO☒

4.13.2 La Proponente cripta i dati custoditi all'interno delle banche dati informatiche? SI☐ NO☒

4.13.3 La Proponente cripta le informazioni in uscita? SI☒ NO☐

4.14 La proponente impone un processo di aggiornamento dei software che includa l'installazione delle relative patch? SI☒ NO☐

Se si:

4.15.1 Le patch critiche sono installate entro 30 giorni dal rilascio? SI☒ NO☐

4.15 Indicare se la Proponente utilizza ad oggi software o sistemi operativi non più supportati dal produttore SI☒ NO☐

Se si, si prega di fornire maggiori dettagli: si tratta di eccezioni minimali

4.16 Si prega di indicare in che quantità la Proponente dispone dei seguenti dispositivi:

	< 100	**101 - 1000**	**> 1001**
Computer fissi	☐	☐	☐
Dispositivi portatili	☐	☒	☐
Numero di server	☐	☐	☐

Sezione 5. Fornitori e Terze Parti

5.1 La proponente esternalizza parte della gestione delle operazioni o della sicurezza dei propri computer o sistemi di rete? SI☐ NO☒

Se si:

5.1.1 Si prega di indicare quali processi sono esternalizzati a provider esterni di servizi:

Processo dei pagamenti	☐
IT Security	☐
Raccolta dati e/o processo	☐
Call center / Service desk	☐
Operational business process	☐
Altro *(specificare sotto)*	☐

5.1.2 Si prega di indicare secondo quale modalità vengono gestiti i data center:

In House	☒
Esternalizzati in Host	☐
Esternalizzati in Cloud	☐

5.2 La Proponente esige che i fornitori siano in possesso di policy e procedure di sicurezza adeguate? SI☒ NO☐

5.3 La Proponente richiede ai fornitori di sottoscrivere una polizza per l'assicurazione della RC professionale o una polizza di RC per la protezione dei dati? SI☐ NO☒

5.4 La proponente richiede ai terzi fornitori di essere mantenuta indenne per eventuali responsabilità derivanti dalla divulgazione di dati personali e/o informazioni confidenziali da parte di terzi? SI☒ NO☐

5.5 Indicare se la Proponente contrattualizza un Service Level Agreement (SLA) con terzi fornitori in grado di facilitare il monitoraggio degli incidenti, il reporting e le azioni per mitigare i danni SI☒ NO☐

SI☒ NO☒

5.6 Indicare se la Proponente permetta ai propri fornitori di servizi IT oppure ai propri dipendenti di accedere dall'esterno alle proprie infrastrutture dati e IT

Sezione 6. Interdipendenza IT e piani di emergenza

6.1 Indicare se la Proponente ha implementato, testato e gestito piani di emergenza IT e di emergenza aziendale

SI☒ NO☐

Fornire dettagli riguardo attuali o futuri impegni per la realizzazione di piani di emergenza all'interno dell'organizzazione: DR Plan e Organizzazione del Disaster

6.2 Si prega di indicare quali tipi di test sono stati svolti o sono programmati:

Table Top Testing	☐	Data dell'ultimo test: Fare clic qui per immettere testo.
Simulazione	☒	Data dell'ultimo test: Fare clic qui per immettere testo.
Test di interruzione parziale	☐	Data dell'ultimo test: Fare clic qui per immettere testo.
Test di interruzione totale	☐	Data dell'ultimo test: Fare clic qui per immettere testo.

6.3 Si prega di indicare quale tipo di misure di emergenza la Proponente ha installato:

Accordi reciproci	☐	Data di ultima attivazione: Fare clic qui per immettere testo.
Cold Standby Site	☐	Data di ultima attivazione: Fare clic qui per immettere testo.
Hot Standby Site	☐	Data di ultima attivazione: Fare clic qui per immettere testo.
Continuous Replication Sites	☒	

Si prega di fornire dettagli riguardo qualsiasi di queste misure di emergenza sia stata esternalizzata: nessuna

6.4 Si prega di indicare il tempo dopo il quale l'impossibilità per i vostri dipendenti / appaltatori di accedere ai sistemi informatici della Proponente avrebbe un impatto significativo sulla vostra attività:

Immediatamente ☒	Dopo 4 ore ☐	Dopo 8 ore ☐	Dopo 24 ore ☐	Mai ☐

6.5 Nel caso di interruzione di rete o di guasto del sistema, si prega di indicare se l'impossibilità per i clienti ad accedere ai sistemi informatici della Proponente avrebbe un impatto significativo sulla sua attività:

Immediatamente ☒	Dopo 4 ore ☐	Dopo 8 ore ☐	Dopo 24 ore ☐	Mai ☐

6.6 Nel caso di interruzione di rete o di guasto del sistema, si prega di indicare una stima della massima perdita finanziaria per ogni ora di interruzione:

indicativamente € 40.000,00

Sezione 7. Contenuti multimediali, Website e Social Network

7.1 La proponente dispone di una procedura di risposta ad eventuali reclami che considerino il materiale creato, esposto o pubblicato dalla Proponente come diffamatorio, illegale o in violazione del diritto alla privacy di terzi? SI☒ NO☐

7.2 La proponente dispone di un legale qualificato che vagli tutti i contenuti prima della loro pubblicazione sul sito internet dell'assicurato? SI☒ NO☐

Se si, la vagliatura comprende i seguenti punti:

7.2.1	Violazione della privacy	SI☒ NO☐
7.2.2	Violazione del copyright	SI☒ NO☐
7.2.3	Violazione del marchio	SI☒ NO☐
7.2.4	Problematiche di denigrazione	SI☒ NO☐

Se no, si prega di descrivere le procedure per evitare la pubblicazione di contenuti impropri o illegali: Fare clic qui per immettere testo.

7.3 La Proponente dispone di un sito internet aziendale? SI☒ NO☐

Se si, sono previste:

7.4.1	Procedure di opt in / opt out durante la raccolta di informazioni personali degli utenti?	SI☒ NO☐
7.4.2	Procedure per la tracciabilità dei visitatori (cookies, ecc.)	SI☒ NO☐

7.4 La Proponente dispone di profili su Social Network? SI☒ NO☐

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

Sezione 8. Sinistri e circostanze

8.1 La Proponente è a conoscenza di perdite, smarrimenti o divulgazioni di dati personali in suo possesso, custodia o controllo, o da parte di chiunque se ne occupi per conto della Proponente nei tre anni precedenti a questa richiesta? SI☒ NO☐

Se si, si prega di fornire dettagli di ciascun reclamo, accusa o episodio, includendo costi, perdite o danni subiti o pagati, e gli importi pagati come perdita sotto qualsiasi polizza assicurativa: Nel periodo indicato ci sono stati casi di infezione da Ransomware su diverse postazioni sia Sogei sia dei propri Clienti, che hanno bloccato la postazione, richiedendo il supporto tecnico per il riprisitno. In nessun caso sono stati persi dati poiché tutti risiedevano su server centralizzati disponibili per il ripristino.

8.2 Negli ultimi tre anni, la Proponente ha mai ricevuto lamentele o richieste di cessione o sospensione in seguito a violazioni di marchi registrati, copyright, privacy o diffamazione riguardo a qualsiasi contenuto pubblicato, esposto o distribuito da o per conto della Proponente? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli sulle richieste ricevute: Fare clic qui per immettere testo.

8.3 La Proponente è mai stata oggetto di azioni investigative riguardo a una presunta violazione di qualsiasi legge sulla privacy? SI☒ NO☐

Se si, si prega di fornire dettagli di ciascun azione o investigazione: Nel periodo di tempo indicato Sogei è stata oggetto di due ispezioni da parte dell'Autorità Garante per la Protezione dei dati personali, realtivamente a due eventi che non ricadono nel punto 8.5, non essendo riconducibili ad attacchi o violazioni. La prima riguardava un servizio erogato per Clienti, ed era stata identificata da una segnalazione proveniente da un ricercatore di sicurezza che evidenziava una possibilità di accedere a dati di altri utenti dello stesso servizio. La seconda riguardava una segnalazione diffusa dalla stampa di una funzionalità di un servizio erogato per un Cliente, che analogamente permetteva di visualizzare dati relativi ad altri utenti e pratiche

dello stesso servizio, da parte di utenti terzi rispetto a quei dati.

8.4 La Proponente ha mai subito un tentativo di estorsione dei suoi sistemi informatici? SI☒ NO☐

Se si, si prega di fornire maggiori dettagli: Nel corso del periodo indicato si sono riscontrati eventi di infezione da Ransomware, legati a postazioni di lavoro di dipendenti Sogei e di utenti dei Clienti. Il Ransomware è una tipologia di virus che cifra i dati sulla postazione e chiede un pagamento per la loro decifratura. Le postazioni sono state tutte cancellate e ripristinate da zero, non sono stati colpiti dati poiché presenti su backup centralizzati.

8.5 La Proponente ha subito intrusioni note (ad esempio accessi non autorizzati o violazioni della sicurezza) o attacchi DDoS ai propri sistemi informatici nei tre anni precedenti a questa richiesta? SI☒ NO☐

Se si, si prega di descrivere le intrusioni o attacchi, compresi eventuali danni causati da tali intrusioni, fornendo indicazioni su tempo perso, ricavi persi, spese per riparare i danni ai sistemi o per ricostruire i database o i software: Ci sono stati diversi attacchi di tipo DDOS nel periodo indicato su alcuni sistemi di Clienti gestiti da Sogei. Gli eventi non hanno comportato danni relativi ai sistemi e sono stati mitigati entro poche ore dall'inizio. Relativamente ad intrusioni si sono verificati due eventi nel corso del 2017 su due servizi di Clienti gestiti da Sogei, in questi casi erano state inserite nel servizio delle pagine non autorizzate, sfruttando vulnerabilità applicative. Non sono stati riscontrati danni ai dati del servizio, e la risoluzione ha richiesto circa un mese.

8.6 La Proponente, le sue controllate o gli amministratori, Dirigenti, Funzionari, dipendenti o altro potenziale assicurato sono a conoscenza o in possesso di informazioni su qualsiasi fatto, circostanza, situazione, evento o operazione che potrebbero dar luogo ad una richiesta di rimborso ai sensi dell'assicurazione qui proposta? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.

Sezione 9. Precedenti Assicurazioni

9.1 La Proponente è attualmente in possesso di una polizza che copra danni tecnologici, violazione della privacy o sicurezza della rete? SI☒ NO☐

Se si, si prega di fornire le seguenti informazioni:

Assicuratore:	Sez. cyber nella Polizza RC Professionale I° Rischio Zurich Sez. Cyber nella polizza RC Profesisonale II° rischio Lloyd's
Massimale aggregato annuo:	I° rischio

	10.000.000 per eventi successivi a retroattività recente 10.000.000 per intero periodo (3anni) per eventi successivi a retroattività remota II° rischio € 15.000.000 per eventi successivi a retroattività recente € 15.000.000 per intero periodo (3 anni) eventi successivi a retroattività remota In eccesso alla polizza I° rischio
Franchigia:	I° rischio € 30.000 per sinistro II° rischio € 30.000
Durata della polizza.	31.12.2015 - 31.12.2018
Premio:	Sez.cyber Polizza RC Professionale I° rischio € 348.412,00 Sez. cyber Polizza RC Professionale II° rischio € 97.800,00
Retroattività	Recente 31.12.2013 Remota 31.12.2002

9.2 La Proponente si è mai vista rifiutare o cancellare una polizza che copra danni tecnologici, violazione di privacy o di sicurezza della rete? SI☐ NO☒

Se si, si prega di fornire maggiori dettagli: Fare clic qui per immettere testo.