QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI 2021

Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

DATI GENERALI CLIENTE E ATTIVITÀ SVOLTA

DATI ANAGRAFICI

Denominazione – Ragione sociale contraente	AZIENDA DI SERVIZI ALLA PERSONA ISTITUTI MILANESI MARTINITT E STELLINE E PIO ALBERGO TRIVULZIO
Codice Fiscale – Partita IVA contraente	04137830966
Denominazione – Ragione sociale assicurato *(Se diverso)*	
Codice Fiscale – Partita IVA assicurato	
Indirizzo ubicazione del rischio	VIA TRIVULZIO, 15 - MILANO
Presenza di più ubicazioni *(In caso affermativo, allegare al presente questionario l'elenco delle altre ubicazioni)*	
Indirizzo web	WWW.ILTRIVULZIO.IT

DATI ATTIVITÀ

Codice Ateco	861040
Data inizio attività	
Numero totale dei dipendenti	1060
Numero di dipendenti che non accedono alla rete aziendale	/
Valore apparecchiature elettroniche	€ 580.000,00 (gli addetti medici non vengono valorizzati poiché non sono connessi alla rete aziendale)
Valore strumenti IoT e sistemi Scada unitamente ai sistemi fisici a cui si applicano	/
Profitto lordo ultimo esercizio **Per profitto lordo s'intende: la differenza fra l'ammontare del volume di affari annuo addizionato alle rimanenze finali e l'ammontare delle rimanenze iniziali addizionato agli altri costi variabili di esercizio non assicurati. Le rimanenze iniziali e quelle finali devono essere determinate secondo i normali metodi contabili dell'assicurato. Ove possibile, compilare l'allegato prospetto analitico denominato "DETERMINAZIONE DEL PROFITTO LORDO AI FINI ASSICURATIVI".*	*Da compilare solo in caso di garanzia Business Interruption* /
Fatturato ultimo esercizio *(Allegare l'ultimo bilancio disponibile)*	€ 71.134.148,00
Indicare la distribuzione geografica del fatturato dell'ultimo esercizio (%)	*Unione Europea* 100 % *USA – Canada* *Resto del mondo*
Previsione di fatturato prossimo esercizio	€ 80.500.000,00

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI 2021

Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

DATI ATTIVITÀ

Indicare la distribuzione geografica del fatturato previsto per il prossimo esercizio (%)	*Unione Europea* 100 % *USA/Canada* *Resto del mondo*

DESCRIZIONE ATTIVITÀ

Descrivere nel dettaglio l'attività svolta

SOCIO SANITARIA ASSISTENZIALE RIABILITATIVA ED EDUCATIVA

MODALITÀ DI PAGAMENTO

Attività di vendita attraverso E-Commerce	☐ Sì ☒ No In caso affermativo, indicare il fatturato (%) derivante da vendite effettuate tramite E-commerce negli ultimi 12 mesi
Accettati pagamenti con carta di credito per beni e servizi	☒ Sì ☐ No
Conformità Payment Card Industry Data Security Standards – PCI DSS	☐ Soggetta ☒ Non soggetta ☐ Conforme

Sono processati pagamenti per conto terzi, comprese transazioni E-commerce?

☐ Sì ☒ No

In caso affermativo, indicare

Nominativi dei terzi	*Volume delle transazioni per terzo all'anno*

SITUAZIONE SINISTRI

Sinistri accaduti negli ultimi 3 anni ai sensi della polizza Cyber?	☐ Sì ☒ No
In caso affermativo, la violazione ha riguardato:	

Violazione della privacy, divulgazione non autorizzata o perdita di informazioni riservate

☐ Sì ☐ No

In caso affermativo, indicare:

Tipologia	*Impatto economico*

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI 2021

Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

SITUAZIONE SINISTRI

Reclami e/o segnalazioni da parte degli interessati ☐ Sì ☒ No	
In caso affermativo, indicare	
Tipologia	*Impatto economico*
Violazione del sistema informatico (attacchi informatici, intrusioni, violazioni della rete o simili) ☐ Sì ☒ No	
In caso affermativo, indicare	
Tipologia	*Impatto economico*
Interruzione di servizio non programmata ☐ Sì ☒ No	
In caso affermativo, indicare:	
Durata di ogni singola interruzione	*Impatto economico*
L'Ente ha subìto dei controlli e delle visite ispettive in materia privacy da parte dell'Autorità?	☐ Sì ☒ No In caso affermativo, indicare l'esito dell'ispezione

MAPPATURA DEGLI ASSET AZIENDALI

Indicare il numero dei computer fissi	☐ <100 ☒ 101-1000 ☐ >1001
Indicare il numero dei device mobili utilizzati	Tablet ☒ <100 ☐ 101-1000 ☐ >1001
	Smartphone ☒ <100 ☐ 101-1000 ☐ >1001
	Laptop ☒ <100 ☐ 101-1000 ☐ >1001

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI 2021

Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

MAPPATURA DEGLI ASSET AZIENDALI

Indicare i sistemi operativi utilizzati sui client fissi/laptop	☒ Precedenti a Windows 10 ☒ Windows 10 ☐ Mac ☐ Linux ☐ Altro
Indicare i sistemi operativi utilizzati su tablet e/o smartphone	☒ Android ☒ IOS
Indicare il numero dei server	☐ <10 ☒ <100 ☐ 101-1000 ☐ >1001
Indicare le modalità di gestione dei data center	☒ In house ☒ Esternalizzati in hosting/housing ☒ In cloud
Indicare i sistemi operativi utilizzati sui server	☐ Precedenti a Windows 2008 R2 ☒ Windows 2008 R2 o superiore ☒ Linux ☐ Altro

OUTSOURCERS

Quali processi relativi alla gestione delle operazioni e/o della sicurezza dei dispositivi e dei sistemi di rete sono esternalizzati a provider esterni di servizi?

Attività	*Fornitore*
☒ Desktop management	FAST WEB SPA
☒ Server management	FASTWEB SPA
☒ Network management	FASTWEB SPA
☐ Security management	
☐ Data center hosting	
☐ Data processing	
☐ Application management	
☐ Alert log monitoring	
☒ Offsite backup e storage	FASTWEB SPA
☐ Co- location facility	
☐ Application service provider (ASP)	
☒ Call center – Service desk	FASTWEB SPA
☐ Operational business process	
☐ Sistemi di pagamento	
☐ Altro (specificare)	

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI 2021

Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

SERVIZI IN CLOUD

Sono utilizzati dei servizi in Cloud?

☒ Sì ☐ No

In caso affermativo, indicare:

Partner	*Servizi*	*Nazione in cui sono conservati i dati*
ADVENIAS SRL	CARTELLA CLINICA	ITALIA
TIM SPA	POSTA ELETTRONICA GOOGLE APPS	UNIONE EUROPEA

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

SICUREZZA DEI SISTEMI, DELLA RETE E DELLE INFORMAZIONI

POLITICA DI SICUREZZA	Q.1	L'Ente ha ottenuto una certificazione ISO/IEC 27001?	☐ Sì ☒ No In caso affermativo, indicare la data dell'ultimo aggiornamento e il perimetro a cui si applica la certificazione
	Q.2	La direzione ha definito, approvato e pubblicato una Politica di Sicurezza delle Informazioni?	☐ Sì ☐ No
	Q.3	Le regole espresse dalla politica di Sicurezza delle Informazioni sono conosciute e accettate formalmente da tutto il personale?	☐ Sì ☐ No
	Q.4	La Politica di sicurezza è periodicamente riesaminata ed aggiornata?	☐ Sì ☐ No
	Q.5	È stato chiaramente identificato e formalizzato il ruolo di Responsabile della Sicurezza Informatica?	☐ Sì ☐ No
	Q.6	L'Ente si è dotata di una funzione interna di Audit che si occupa di verificare e garantire la corretta implementazione dei presidi di sicurezza informatica, comprese le Policy adottate dall'Ente?	☐ Sì ☐ No
RISORSE UMANE	Q.7	L'Ente prevede dei cicli di formazione specifici sui temi di Information Security (con cadenza almeno annuale) per garantire la consapevolezza, l'istruzione e l'addestramento dei collaboratori in relazione al ruolo che ricopriranno?	☐ Sì ☒ No
	Q.8	È presente una procedura che, durante le fasi di conclusione del rapporto lavorativo, preveda un immediato recupero degli elementi di sicurezza (chiavi, tessere e simili), la restituzione degli asset in dotazione e una contestuale disabilitazione delle utenze?	☒ Sì ☐ No
GESTIONE DEGLI ASSET, REMOTE CONTROL E SMART	Q.9	L'Ente ha implementato un processo di ICT Asset Management, che identifichi tutti gli asset informativi (client, server, apparati di rete, Scada, IoT, device mobili, applicazioni dati e simili) oggetto della copertura assicurativa, nonché l'ownership e le relative responsabilità?	☒ Sì ☐ No
	Q.10	L'Ente ha definito, formalizzato e condiviso con i tutti i suoi collaboratori, delle specifiche istruzioni per un corretto utilizzo degli asset (a.e. e-mail, internet, social media, supporti rimovibili, regole di comunicazione telefonica, regole di utilizzo laptop in ambienti pubblici, utilizzo di servizi di rete e simili)?	☒ Sì ☐ No

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

GESTIONE DEGLI ASSET, REMOTE CONTROL E SMART WORKING	Q.11	L'Ente ha implementato, sui dispositivi aziendali utilizzabili all'esterno dell'azienda, misure di sicurezza equivalenti a quelle degli asset presenti nel perimetro aziendale (es. antivirus, aggiornamenti, cambio password, cifratura, backup dei dati)?	☒ Sì ☐ No In caso affermativo, indicare i dispositivi sui quali sono applicate le misure di sicurezza ☒ Laptop ☐ Tablet ☐ Smartphone
	Q.12	L'Ente ha attivato modalità di lavoro agile - smart working?	☐ Sì con BYOD ☒ Sì senza BYOD ☐ No
	Q.13	Esistono procedure per verificare preventivamente i requisiti e le configurazioni di sicurezza degli asset informatici personali nel caso in cui un collaboratore utilizzi un proprio dispositivo all'interno del perimetro aziendale (BYOD)?	☒ Sì ☐ No
	Q.14	L'Ente adotta modalità di deployment differenziando le attivazioni su pc aziendali da quelle in BYOD?	☐ Sì ☒ No
	Q.15	L'Ente ha reso ai propri collaboratori delle specifiche istruzioni sulle modalità di lavoro in smart working in cui sono dettagliate le basi della sicurezza nel lavoro da remoto?	☒ Sì ☐ No
	Q.16	Per le attivazioni su device aziendali, sono state implementate le seguenti misure di sicurezza?	☐ Disk Encryption ☐ DLP ☐ MDM (Mobile Device Management) ☐ AV con firewall ☒ Connessione con VPN con 2FA (OTP - authenticator) ovvero altra modalità di connessione attivata (a.e. accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)
	Q.17	Per le attivazioni in BYOD, sono state implementate le seguenti misure di sicurezza?	☐ Rilascio di agent sulle macchine degli users ☐ Revoca privilegi amministratore ☐ Verifica presenza AV con firewall con preventiva scansione ☐ Rilascio di soluzione di connessione con VPN con 2FA (OTP - authenticator) ovvero altra modalità di connessione attivata (a.e. accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

CONTROLLO DEGLI ACCESSI	Q.18	L'Ente definisce una politica di controllo degli accessi basata sul principio del privilegio minimo?	☒ Sì	☐ No
	Q.19	La politica di controllo accessi prevede una fase di riesame periodico dei diritti di accesso degli utenti e degli amministratori di sistema?	☒ Sì	☐ No
	Q.20	L'Ente provvede a fornire un identificativo univoco e vieta l'utilizzo di identificativi o utenze condivise (anche a livello di amministratore di sistema)?	☐ Sì	☒ No
	Q.21	L'Ente si è dotata di un processo formale per l'assegnazione e revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi (inclusi i diritti di accesso privilegiato)?	☒ Sì	☐ No
	Q.22	L'Ente ha implementato e diffuso una password policy che garantisca e applichi un adeguato livello di complessità e robustezza?	☒ Sì	☐ No

CONTROLLI CRITTOGRAFICI	Q.23	L'Ente ha implementato delle soluzioni crittografiche e adottato una policy relativa alla definizione dei requisiti minimi di sicurezza e di controllo delle tecnologie adottate (es. uso, protezione e durata delle chiavi di crittografia)?	☐ Sì	☒ No

SICUREZZA FISICA	Q.24	Il perimetro fisico dell'impianto e/o degli uffici è chiaramente delimitato e ogni singolo varco è presidiato da operatori di sicurezza e/o impianti di rilevazione accessi?	☒ Sì ☐ No
	Q.25	Sono previsti dei sistemi di verifica e/o registrazione e/o tracciatura in ingresso dei visitatori che accedono al building e/o alla struttura e/o all'impianto, anche attraverso l'esibizione di un documento di identità?	☐ Sì ☒ No
	Q.26	Gli accessi sono chiusi e presidiati al di fuori dell'orario di lavoro?	☐ Sì ☒ No
	Q.27	L'accesso ai locali del datacenter è permesso solo al personale autorizzato, dotato di credenziali e/o badge specifici?	☒ Sì ☐ No
	Q.28	Sono presenti dei sistemi di controllo degli accessi al data center? Specificare quali	☒ Apparati CCTV ☐ Bussole di accesso degli edifici con metal detector ☐ Sensori anti-intrusione e dissuasori veicolari ☐ Sistemi tecnologici anti-tailgating ☒ Sensori volumetrici ☒ Lettori badge e/o password e/o chiavi elettroniche (anche con doppi sistemi di autenticazione) ☐ Sistema di acquisizione delle impronte digitali con rilevamento di impronta falsa ☐ Altro (specificare)

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

SICUREZZA FISICA	Q.29	Le operazioni di manutenzione da parte dei fornitori all'interno del data center in house sono sempre supervisionate da personale interno?	☒ Sì ☐ No
	Q.30	Esiste una procedura di revisione periodica degli accessi al building e/o all'infrastruttura e/o al data center (log controllo accessi o revisione dei registri cartacei)?	☐ Sì ☒ No
	Q.31	Caratteristiche del data center	☒ Rack e i server presenti all'interno del data center prevedono sempre una ridondanza delle linee elettriche ☒ Il sistema di condizionamento è correttamente dimensionato e dotato di sistemi automatici di rilevamento e allerta di temperatura e umidità ☒ Sistemi di controllo antifumo e di rilevazione di sicurezza ambientale (a.e. sensori per pavimento flottante) ☒ UPS ☒ Il sistema di cablaggio strutturato è conforme alle normative di settore ☐ Altro (specificare)

SICUREZZA DELLE ATTIVITÀ OPERATIVE	Q.32	[Change Management] Le fasi di change management prendono sempre in considerazione i requisiti di sicurezza e i criteri di accettazione per nuove versioni o sistemi?	☒ Sì ☐ No
	Q.33	[Change Management] Gli ambienti di sviluppo, test e produzione sono separati per ridurre il rischio di accesso o cambiamenti non autorizzati all'ambiente di produzione?	☒ Sì ☐ No
	Q.34	[Anti-malware] L'Ente si è dotata di un sistema centralizzato, regolarmente aggiornato (almeno mensile), per la gestione dei sistemi antivirus e/o anti-malware che copre tutti gli asset rientranti della copertura assicurativa?	☒ Sì ☐ No
	Q.35	[Anti-malware] L'Ente pianifica ed esegue scansioni periodiche su tutti gli asset informatici che sono oggetto della copertura assicurativa?	☒ Sì ☐ No
	Q.36	[Anti-malware] Le impostazioni del software antivirus e/o anti-malware sono impostate per scansionare anche gli allegati di posta e il contenuto delle pen drive quando utilizzate?	☒ Sì ☐ No
	Q.37	[Backup] Con quale frequenza è eseguito il back up dei dati?	GIORNALIERO
	Q.38	[Backup] Quale modalità di salvataggio e recupero dati fa parte della strategia di back up scelta?	☒ Back up completo ☐ Back up differenziale ☒ Back up incrementale
	Q.39	[Backup] L'Ente si è dotato di una procedura di backup che identifica le informazioni critiche per il business?	☒ Sì ☐ No

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

SICUREZZA DELLE ATTIVITÀ OPERATIVE	**Q.40**	[Backup] Dove sono salvate le copie di back up?	☒ Supporti esterni (Server o NAS, chiavette USB, dischi esterni, e simili) ☐ Cloud
	Q.41	[Backup] Le copie di back up salvate su supporti esterni, sono conservate in siti alternativi e/o secondari per garantire l'efficacia dei processi di Disaster Recovery?	☒ Sì ☐ No
	Q.42	[Backup] Vengono eseguiti periodicamente test di ripristino, in particolare dei database che sono oggetto della copertura assicurativa?	☒ Sì ☐ No
	Q.43	[Backup] Le copie di backup vengono protette in base al livello di confidenzialità delle informazioni che contengono?	☐ Sì ☒ No
	Q.44	[Backup] Vengono eseguiti i backup delle configurazioni degli apparati di rete (a.e. router, firewall e simili)?	☒ Sì ☐ No
	Q.45	[Raccolta Log & Monitoraggio] L'Ente definisce a priori quali log sono ritenuti essenziali per identificare eventuali anomalie e/o evidenziare potenziali attacchi e/o azioni malevole sui propri applicativi e infrastrutture "mission critical"?	☐ Sì ☒ No
	Q.46	[Raccolta Log & Monitoraggio] Per garantire una corretta registrazione degli eventi, l'orario interno dei sistemi è sincronizzato con i time server tramite protocollo NTP (Network Time Protocol)?	☒ Sì ☐ No
	Q.47	[Raccolta Log & Monitoraggio] L'Ente si è dotata di sistema di correlazione e gestione dei log che supporta le funzioni interne e/o security nell'identificazione e nell'analisi degli eventi ritenuti critici, anche in ottica forense?	☐ Sì ☒ No
	Q.48	[Raccolta Log & Monitoraggio] L'accesso ai file di log è consentito solo a soggetti individuati nel rispetto del principio "need to know" prevedendo, con granularità, i profili delle utenze che possono accedere e i relativi privilegi?	☒ Sì ☐ No
	Q.49	[Raccolta Log & Monitoraggio] L'Ente si è dotato di un sistema di Log Management in grado di monitorare gli accessi eseguiti dagli amministratori e dagli operatori di sistema sui sistemi aziendali?	☒ Sì ☐ No
	Q.50	[Raccolta Log & Monitoraggio] Quali misure di protezione sono state adottate dall'Ente per assicurare l'inalterabilità dei Log?	☒ Accesso fisico controllato per le aree contenenti gli apparati di gestione dei log ☐ Accesso logico ai dati tramite 2FA- two factor authentication ☐ Crittografia dei file durante la conservazione ☐ Altro (specificare)
	Q.51	[Raccolta Log & Monitoraggio] Indicare le tempistiche di conservazione dei file di log stabilite dall'Ente	☒ < 6 mesi ☐ ≥ 6 mesi ☐ ≥ 12 mesi ☐ Altro (specificare)

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

SICUREZZA DELLE ATTIVITÀ OPERATIVE	Q.52	Sono attuate procedure per controllare l'installazione di software sui sistemi gestiti?	☐ Sì	☒ No
	Q.53	[Gestione vulnerabilità tecniche] L'Ente effettua, su tutti gli asset rientranti nel perimetro, dei test di sicurezza periodici (a.e. Vulnerability Assessment, penetration test) e attività di Risk Analysis?	☐ Sì	☒ No In caso affermativo, descrivere le principali criticità emerse

SICUREZZA DELLE RETI	Q.54	L'Ente dispone di sistemi firewall aggiornati?	☒ Sì	☐ No
	Q.55	È attivo un monitoraggio in tempo reale sulle anomalie?	☒ Sì	☐ No
	Q.56	L'Ente si è dotato di sistemi di intrusion detection e/o prevention (IDS/IPS), costantemente aggiornati?	☐ Sì	☐ No
	Q.57	Le connessioni di telecomunicazione adottano sistemi di ridondanza per garantire continuità operativa?	☒ Sì	☐ No
	Q.58	In relazione alle informazioni scambiate su reti pubbliche, viene garantito un adeguato livello di cifratura del canale (a.e. adozione di protocolli di tunelling in SSL o SSH) o delle informazioni trasmesse?	☒ Sì	☐ No
	Q.59	L'Ente ha segregato la rete interna (LAN) in Virtual LAN (VLAN) o domini in base al livello di sicurezza dei processi e informazioni gestite?	☒ Sì	☐ No

FORNITORI ESTERNI	Q.60	L'Ente si è dotato di un sistema di selezione dei fornitori che valuti, oltre alla loro solidità finanziaria, anche le loro politiche di cyber security e di trattamento dei dati, e che includa una verifica periodica sul mantenimento dei requisiti richiesti in ingresso?	☒ Sì	☐ No
	Q.61	Per i fornitori esiste una procedura di autorizzazione all'accesso diretto o da remoto ai sistemi, che prevede una verifica periodica e una revoca superato un periodo di tempo prestabilito?	☒ Sì	☐ No
	Q.62	I fornitori di servizi cloud sono in possesso di certificazioni professionali (a.e. CCSP Certified Cloud Security Professional, EXIN Cloud Computing Foundation, EC Council CAST 618 Designing and Implementing Cloud Security, e simili)?	☒ Sì	☐ No

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI INFORMATIVI	Q.63	L'Ente adotta controlli di adeguatezza, conformità e sicurezza rispetto a software e/o sistemi informativi sviluppati da terze parti?	☐ Sì	☒ No
	Q.64	L'accesso agli ambienti di sviluppo, pre-produzione e produzione è consentito attraverso l'utilizzo di account diversi per ogni ambiente?	☐ Sì	☒ No
	Q.65	Sono eseguite periodicamente le manutenzioni programmate richieste dalle specifiche dei produttori?	☒ Sì	☐ No

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

CONTINUITÀ OPERATIVA	**Q.66**	L'Ente ha implementato un processo documentato di Business Impact Analysis (BIA) regolarmente aggiornato che identifichi gli impatti in termini di tempi di interruzione, danni (a.e. patrimoniali diretti e indiretti) e relativi tempi di ripristino?	☐ Sì ☒ No
	Q.67	L'Ente si è dotata di un piano di ripristino o Business Continuity Plan (BCP) integrato con procedure operative e istruzioni di ripristino dettagliate?	☐ Sì ☒ No
	Q.68	L'Ente identifica e definisce in un Disaster Recovery Plan tutte le attività di ripristino tecnico?	☐ Sì ☒ No
	Q.69	Sono testati regolarmente	☐ Il piano di business continuity ☐ Il piano di disaster recovery
	Q.70	L'Ente ha adottato procedure di valutazione degli impatti che eventuali cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi, possono avere sulla sicurezza delle informazioni?	☐ Sì ☒ No
	Q.71	Si coinvolgono i fornitori nei test di continuità operativa?	☐ Sì ☒ No
	Q.72	Si prega di valutare, in caso di interruzione di rete o di guasto del sistema, dopo quanto tempo, l'impossibilità di accedere ai sistemi informatici, genererebbe un impatto significativo sull'attività	
		Attività (o settori)	*Massimo periodo di interruzione prima di avere un impatto negativo*
		CARTELLA CLINICA ACCETTAZIONE RICOVERI DIMISSIONI RICOVERI	☒ Immediatamente ☐ > 4ore ☐ > 12ore ☐ > 24ore ☐ > 48 ore ☐ > 5 giorni ☐ Mai
		VISITE SPECIALISTICHE	☒ Immediatamente ☐ > 4ore ☐ > 12ore ☐ > 24ore ☐ > 48 ore ☐ > 5 giorni ☐ Mai

[redacted]		CONTABILITA'	☐ Immediatamente ☐ > 4ore ☒ > 12ore ☐ > 24ore ☐ > 48 ore ☐ > 5 giorni ☐ Mai
		GESTIONE RISORSE UMANE	☐ Immediatamente ☐ > 4ore ☒ > 12ore ☐ > 24ore ☐ > 48 ore ☐ > 5 giorni ☐ Mai
	Q.73	Indicare, in caso di interruzione di rete o guasto di sistema, una stima della massima perdita finanziaria per ogni ora di interruzione	

GESTIONE INCIDENTI	Q.74	L'Ente ha implementato un processo di Incident Management/Response (persone, ruoli, responsabilità)?	☐ Sì ☒ No
	Q.75	Esistono playbook (elenchi azioni predefinite) in funzione del tipo di incidente occorso (a.e.. sospensione cautelativa del sistema colpito, cambio password e simili)?	☐ Sì ☒ No

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

GESTIONE DEI DATI PERSONALI

GESTIONE DELLE ESPOSIZIONI PRIVACY

Q.76	Nell'esercizio della propria attività, che tipo di dati personali raccoglie, processa o conserva l'Ente?		
	Tipologia dei dati trattati	*Volume dei dati trattati*	
	☑ Dati finanziari (carte di credito e/o debito e/o conto corrente)	☐≤100 ☐≤1.000 ☑≤100.000 ☐≤1.000.000 ☐≥1.000.000	
	☑ Dati personali di terzi soggetti	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☑≥1.000.000	
	☑ Informazioni sanitarie	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☑≥1.000.000	
	☑ Proprietà intellettuale e/o copyrights e/o segreti commerciali	☑≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000	
Q.77	L' Ente ha implementato un sistema di gestione dei dati adempiendo alle prescrizioni previste dalla normativa nazionale ed europea in materia di trattamento dei dati e nel rispetto dei diritti degli interessati? **Si intendono incluse le misure che soddisfino i principi di privacy by design e privacy by default, quali ad esempio: ridurre al minimo il trattamento dei dati, offrire trasparenza per quanto riguarda i trattamenti (a.e. prevedendo delle informative conformi da rendere prima di raccogliere i dati), raccolta del consenso informato prima di procedere a determinati trattamenti (a.e.. marketing) e simili*	☑ Sì ☐ No	
Q.78	Indicare le misure organizzative implementate per l'adeguamento alla normativa nazionale ed europea in materia di trattamento dei dati	☑ Aggiornamento informative (dipendenti, clienti, sito internet - inclusa Cookie Policy, e simili) ☑ Periodiche sessioni di formazione per dipendenti in materia privacy ☑ Processo di raccolta e gestione di consensi informati ☑ Tutele rafforzate nel trattamento di categorie particolari di dati (a.e. informazioni sanitarie) ☑ Redazione e aggiornamento registro dei trattamenti ☑ Aggiornamento nomine per il trattamento dei dati (incaricati al trattamento, responsabili, amministratori di sistema e simili) ☐ Trasferimento dati extra UE nel rispetto delle condizioni dalla normativa (art. 44, 45 e 46 GDPR) ☐Altro	

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)

Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

GESTIONE DELLE ESPOSIZIONI PRIVACY	**Q.79**	Quali delle seguenti Policy (nelle quali sono anche definiti ruoli e responsabilità) sono state adottate dall'Ente?	☒ Data Breach IN CORSO DI ADOZIONE ☐ Data Retention (nella quale sono stati stabiliti i termini di conservazione e relativa cancellazione dei dati per tutti i trattamenti) ☐ Gestione delle richieste degli interessati in materia privacy ☒ Regolamento sul corretto utilizzo dei sistemi informatici aziendali ☐ Altro (specificare)
	Q.80	A chi è attribuita l'attività di gestione della privacy dell'Ente?	☐ Società di consulenza o studio legale ☒ Ufficio privacy all'interno dell'azienda (Privacy manager) ☐ Libero professionista
	Q.81	L'Ente ha nominato un Responsabile della protezione dei dati (DPO)?	☒ Sì ☐ No ☐ Non soggetta
	Q.82	L'Ente effettua i seguenti trattamenti	☐ Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive (a.e. screening dei propri clienti utilizzando database di rischio creditizio e/o lotta alle frodi e/o riciclaggio e finanziamento del terrorismo (AML/CTF), creazione di profili comportamentali /marketing a partire dalla navigazione sul proprio sito e simili) ☐ Decisioni automatizzate che producono significativi effetti giuridici sull'interessato (a.e. selezione candidati tramite algoritmo) ☐ Utilizzo nuove soluzioni tecnologiche e organizzative (a.e. associazione di tecniche dattiloscopiche e riconoscimento del volto per il controllo degli accessi fisici) ☐ Monitoraggio regolare e sistematico (a.e. sorveglianza sistematica di un'area accessibile al pubblico) ☒ Trattamento di dati su larga scala (da valutare in base al numero degli interessati coinvolti, il volume dei dati trattati, la durata delle attività di trattamento o l'estensione geografica del trattamento) ☐ Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (a.e. mobile payment)

GESTIONE DELLE ESPOSIZIONI PRIVACY	**Q.83**	Sono previsti dei sistemi dai quali può derivare un controllo anche a distanza dei dipendenti?	☐ Sì ☒ No In caso affermativo, indicare quali ☐ Sistemi di geolocalizzazione (veicoli) ☐ Videosorveglianza ☐ Monitoraggio della navigazione internet (sistema di log e simili) ☐ Altro
	Q.84	Nel caso in cui l'Ente esegua uno dei trattamenti descritti nei due punti precedenti (Q.82 – Q.83), ha provveduto ad effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) prima di procedere al trattamento?	☐ Sì ☒ No

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

CONTENUTI MULTIMEDIALI

GESTIONE DELLA MULTIMEDIALITÀ	**Q.85**	Di quale tipologia di canali digitali si avvale l'Ente?	☒ Social Network ☐ Blog ☐ Chatroom
	Q.86	Sul sito web aziendale, sono previste	☐ Procedure di doppio opt-in per la raccolta delle informazioni personali degli utenti (a.e. in fase di iscrizione al sito, newsletter e simili) ☐ Procedure di opt out, compreso l'inserimento del link per la disiscrizione al servizio (a.e. newsletter) ☐ Procedure per la tracciabilità e/o profilazione degli utenti/ visitatori (a.e. cookie e simili)
	Q.87	L'Ente esternalizza tutta o solo in parte la propria pubblicità online a terze parti?	☐ Viene esternalizzata tutta la pubblicità online ☐ Viene esternalizzata solo una parte (indicare quale) ☐ No, la pubblicità viene gestita da un ufficio interno all'organizzazione
	Q.88	L'Ente ha adottato delle procedure per impedire la pubblicazione di contenuti diffamatori, illegali o in violazione al diritto alla privacy di terzi sui propri canali online?	☐ Sì ☐ No In caso affermativo, descrivere quali (a.e. ricorso a un legale qualificato)
	Q.89	La vagliatura dei contenuti pubblicati sui canali online dell'Ente, comprende:	☐ Violazione del diritto alla riservatezza ☐ Violazione del copyright ☐ Lesione dell'altrui reputazione ☐ Altro (specificare)
	Q.90	L' Ente dispone di una procedura per rispondere a eventuali reclami sui contenuti creati e pubblicati, considerati calunniosi, illegali o in violazione al diritto alla privacy di terzi?	☒ Sì ☐ No In caso affermativo, descrivere la procedura adottata L'UFFICIO PROTOCOLLO INOLTRA ALL'UFF LA SEGNALAZIONE/RECLAMO E IN CASO DI NECESSITÀ INTERVIENE L'AREA AA.GG.LL.

QUESTIONARIO POLIZZA CYBER RISK ENTI PUBBLICI (FATTURATO > 50 MIO)
Qualora la domanda non sia pertinente all'attività dell'assicurato riportare nel relativo campo la dicitura NON PERTINENTE

	DICHIARAZIONI
	La firma del presente questionario non obbliga il proponente all'acquisto della polizza
	Il sottoscritto dichiara che tutte le dichiarazioni e le informazioni rese con il presente questionario sono vere e che non sussistono fatti materiali errati o sottaciuti. Per fatto materiale si intende un qualsiasi accadimento che potrebbe influenzare l'accettazione o la valutazione del rischio
	Il sottoscritto accetta che il presente questionario, qualsiasi allegato allo stesso o informazione fornita con lo stesso, e tutte le altre informazioni rese e/o richieste, potrebbero costituire la base di un eventuale e futuro contratto di assicurazione. Il sottoscritto conseguentemente si obbliga ad informare l'assicuratore di qualsiasi modifica materiale di qualsiasi informazione, dichiarazione, rappresentazione o fatto presentati in questo questionario, che si verifichino prima o dopo la data di decorrenza della copertura assicurativa
	Il presente questionario è vincolante per e formerà base e parte integrante della polizza di assicurazione dei dati conclusa con l'assicuratore
	Il questionario è soggetto ad approvazione finale da parte dell'assicuratore

Luogo e data Milano, 23/7/2021

Titolo e funzione dell'incaricato

Firma IL RUP
AVV. SABRINA ALLISIO