Sez.1 DATI GENERALI CLIENTE E ATTIVITA' SVOLTA

DATI ANAGRAFICI	Denominazione / Ragione sociale Contraente	TRENTINO DIGITALE SPA
	Cod.Fiscale / Partita IVA Contraente	P.IVA 00990320228
	Denominazione / Ragione sociale Assicurato (se diverso)	
	Cod.Fiscale / Partita IVA Assicurato	
	Indirizzo ubicazione del rischio	VIA GILLI 2 38121 TRENTO
	Presenza di più ubicazioni *(In caso affermativo, allegare al presente questionario l'elenco delle altre ubicazioni)*	VIA PEDROTTI 18 38121 TRENTO
	Indirizzo web	WWW.TRENTINODIGITALE.IT

DATI ATTIVITÀ	Codice Ateco	62.02
	Data inizio attività	01/01/1984
	Numero totale dei dipendenti	AL 30/06/2021 NR 300
	Numero di dipendenti che non accedono alla rete aziendale	ZERO
	Somme assicurate apparecchiature elettroniche	-
	Somma assicurata 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".*	Utile bilancio 2020: euro 988.853
	Fatturato ultimo esercizio *(Allegare l'ultimo bilancio disponibile)*	Euro 52.802.466
	Indicare la distribuzione geografica del fatturato dell'ultimo esercizio (%)	*Unione Europea* _____*100%*_____ *USA/Canada* _____ *Resto del mondo* _____
	Previsione di fatturato prossimo esercizio	
	Indicare la distribuzione geografica del fatturato previsto per il prossimo esercizio (%)	*Unione Europea* _*100%*_____ *USA/Canada* _____ *Resto del mondo* _____
DESCRIZIONE A	Descrivere nel dettaglio l'attività svolta La Società, a capitale interamente pubblico, costituisce lo strumento del sistema della Pubblica Amministrazione del Trentino per la **progettazione**, lo **sviluppo**, la **manutenzione** e l'esercizio del **Sistema Informativo Elettronico Trentino** (S.I.N.E.T.), evoluzione del Sistema Informativo Elettronico Pubblico (S.I.E.P.), e dell'infrastruttura, a beneficio delle Amministrazioni Pubbliche stesse e degli altri enti e soggetti del sistema.	

TIPOLOGIA ATTIVITÀ	

MODALITA' DI PAGAMENTO	Attività di vendita attraverso E-Commerce	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	☐no
	Conformità Payment Card Industry Data Security Standards – PCI DSS	☐soggetta ☐non soggetta ☐ conforme
	Sono processati pagamenti per conto terzi, comprese transazioni E-commerce? ☐si ☐no In caso affermativo, indicare:	
	Nominativi dei terzi	*Volume delle transazioni per terzo all'anno*

SITUAZIONE ASSICURATIVA	Altre polizze in corso con il nostro gruppo ☐ si ☐no In caso affermativo, indicare:	
	Tipologia	*Importo complessivo delle coperture in corso con il nostro gruppo*

SITUAZIONE SINISTRI	Sinistri accaduti negli ultimi 3 anni ai sensi della polizza Cyber	☐ si xno
	In caso affermativo, la violazione ha riguardato:	
	Violazione della privacy, divulgazione non autorizzata o perdita di informazioni riservate ☐si ☐no In caso affermativo, indicare:	
	Tipologia	*Impatto economico*
	Reclami/Segnalazioni da parte degli interessati ☐ si ☐no In caso affermativo, indicare:	
	Tipologia	*Impatto economico*

Questionario Polizza Cyber Risk_Addendum Lotto 3)

	Violazione del sistema informatico (attacchi informatici, intrusioni, violazioni della rete o simili) ☐ si ☐no In caso affermativo, indicare:	
	Tipologia	*Impatto economico*
	Interruzione di servizio non programmata ☐ si ☐no In caso affermativo, indicare:	
	Durata di ogni singola interruzione	*Impatto economico*
	<4h	-
	L'organizzazione ha subìto dei controlli e delle visite ispettive in materia privacy da parte dell'Autorità?	☐ si xno 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
	Indicare i sistemi operativi utilizzati sui client fissi/laptop	Xprecedenti a Windows 10 XWindows 10 XMac XLinux ☐ Altro
	Indicare i sistemi operativi utilizzati su tablet/smartphone	XAndroid ☐IOS
	Indicare il numero dei server	☐ <10 ☐ <100 ☐ 101-1000 X >1001
	Indicare le modalità di gestione dei data center	Xin house Xesternalizzati in hosting/housing Xin cloud
	Indicare i sistemi operativi utilizzati sui server	Xprecedenti a Windows 2008 R2 XWindows 2008 R2 o superiore XLinux X 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*
	X Desktop management	DEXIT
	☐ Server management	
	X Network management	In parte: Sistemi Informativi
	X Security management	In parte: Sistemi Informativi
	☐ Data center hosting	
	☐ Data processing	
	☐ Application management	
	☐ Alert log monitoring	
	☐ Offsite backup e storage	
	☐ Co- location facility	
	☐ Application service provider (ASP)	
	X Call center/Service desk	In parte
	☐ Operational business process	

	☐ Sistemi di pagamento	
	☐ Altro, specificare:	

SERVIZI IN CLOUD	Sono utilizzati dei servizi in Cloud? X si ☐no In caso affermativo, indicare:		
	Partner	*Servizi*	*Nazione in cui sono conservati i dati*
	SPC Cloud TIM	Vari	Italia
	AWS	vari	
	Azure	SAp Hana Test / Sviluppo	

Sez.2			
SICUREZZA DEI SISTEMI, DELLA RETE E DELLE INFORMAZIONI			
POLITICA DI SICUREZZA	**Q.1**	L'organizzazione ha ottenuto una certificazione ISO/IEC 27001?	Xsi ☐no In caso affermativo, indicare la data dell'ultimo aggiornamento e il perimetro a cui si applica la certificazione:
	Q.2	La Direzione Aziendale ha definito, approvato e pubblicato una Politica di Sicurezza delle Informazioni?	Xsi ☐no
	Q.3	Le regole espresse dalla Politica di Sicurezza delle Informazioni sono conosciute e accettate formalmente da tutto il personale?	Xsi ☐no
	Q.4	La Politica di sicurezza è periodicamente riesaminata ed aggiornata?	Xsi ☐no
	Q.5	È stato chiaramente identificato e formalizzato il ruolo di Responsabile della Sicurezza Informatica?	Xsi ☐no
	Q.6	L'organizzazione 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'azienda?	Xsi ☐no
RISORSE UMANE	**Q.7**	L'organizzazione 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 in azienda?	Xsi ☐no
	Q.8	E' presente una procedura che, durante le fasi di conclusione del rapporto lavorativo, preveda un immediato recupero degli elementi di sicurezza (chiavi, tessere etc.), la restituzione degli asset in dotazione e una contestuale disabilitazione delle utenze?	Xsi ☐no
GESTIONE DEGLI ASSET, REMOTE CONTROLLESM	**Q.9**	L'organizzazione 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, etc.) oggetto della copertura assicurativa, nonché l'ownership e le relative responsabilità?	Xsi ☐no
	Q.10	L'organizzazione ha definito, formalizzato e condiviso con i tutti i suoi collaboratori, delle specifiche istruzioni per un corretto utilizzo degli asset aziendali (es. email, internet, social media, supporti rimovibili, regole di comunicazione telefonica, regole di utilizzo laptop in ambienti pubblici, utilizzo di servizi di rete, etc.)?	Xsi ☐no
	Q.11	L'organizzazione 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)?	☐si Xno In caso affermativo, indicare i dispositivi sui quali sono applicate le misure di sicurezza ☐laptop ☐tablet ☐smartphone
	Q.12	L'organizzazione ha attivato modalità di lavoro agile /smart working?	Xsi, con BYOD ☐si, 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)?	☐si Xno
	Q.14	L'organizzazione adotta modalità di deployment differenziando le attivazioni su pc aziendali da quelle in BYOD?	Xsi ☐no
	Q.15	L'organizzazione ha reso ai propri collaboratori delle specifiche istruzioni sulle modalità di lavoro in smart	Xsi ☐no

ARTWORKING		working in cui sono dettagliate le basi della sicurezza nel lavoro da remoto?	
	Q.16	Per le attivazioni su device aziendali, sono state implementate le seguenti misure di sicurezza:	☐disk Encryption ☐DLP ☐MDM (Mobile device Management) XAV con firewall XConnessione con VPN con 2FA (OTP/authenticator) ovvero altra modalità di connessione attivata (es.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 (es.accesso a bolla citrix o altra piattaforma di disintermediazione su pagina crittografata (https) ovvero soluzione di virtual desktop)

CONTROLLO DEGLI ACCESSI	**Q.18**	L'organizzazione definisce una politica di controllo degli accessi basata sul principio del privilegio minimo?	X si ☐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?	X si ☐no
	Q.20	L'organizzazione provvede a fornire un identificativo univoco e vieta l'utilizzo di identificativi o utenze condivise (anche a livello di amministratore di sistema)?	X si ☐no
	Q.21	L'organizzazione 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)?	X si ☐no
	Q.22	L'organizzazione ha implementato e diffuso una password policy che garantisca e applichi un adeguato livello di complessità e robustezza?	X si ☐no

CONTROLLI CRITTOGRAFICI	**Q.23**	L'organizzazione 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)?	Xsi ☐no

SICUREZZA	**Q.24**	Il perimetro fisico dell'impianto / uffici è chiaramente delimitato e ogni singolo varco è presidiato da operatori di sicurezza e/o impianti di rilevazione accessi?	Xsi ☐no
	Q.25	Sono previsti dei sistemi di verifica/registrazione/tracciatura in ingresso dei visitatori che accedono al building / struttura / impianto, anche attraverso l'esibizione di un documento di identità?	Xsi ☐no

FISICA	**Q.26**	Gli accessi sono chiusi e presidiati al di fuori dell'orario di lavoro?	Xsi ☐no
	Q.27	L'accesso ai locali del datacenter è permesso solo al personale autorizzato, dotato di credenziali / badge specifici?	Xsi ☐no
	Q.28	Sono presenti dei sistemi di controllo degli accessi al data center? Specificare quali.	X Apparati CCTV ☐Bussole di accesso degli edifici con metal detector ☐Sensori anti-intrusione e dissuasori veicolari ☐Sistemi tecnologici anti-tailgating ☐Sensori volumetrici X Lettori badge / password / chiavi elettroniche (anche con doppi sistemi di autenticazione) ☐Sistema di acquisizione delle impronte digitali con rilevamento di impronta falsa ☐Altro, specificare
	Q.29	Le operazioni di manutenzione da parte dei fornitori all'interno del data center in house sono sempre supervisionate da personale interno?	X si ☐no
	Q.30	Esiste una procedura di revisione periodica degli accessi al building / infrastruttura / data center (log controllo accessi o revisione dei registri cartacei)?	X si ☐no
	Q.31	Caratteristiche del data center:	X rack e i server presenti all'interno del data center prevedono sempre una ridondanza delle linee elettriche X il sistema di condizionamento è correttamente dimensionato e dotato di sistemi automatici di rilevamento e allerta di temperatura e umidità X sistemi di controllo antifumo e di rilevazione di sicurezza ambientale (es. sensori per pavimento flottante) X UPS X il sistema di cablaggio strutturato è conforme alle normative di settore ☐Altro, specificare_____

SICUREZZA DELLE ATTIVITA' 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?	Xsi ☐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?	Xsi ☐no
	Q.34	[Anti-Malware] - L'organizzazione si è dotata di un sistema centralizzato, regolarmente aggiornato (almeno mensile), per la gestione dei sistemi antivirus/anti-Malware che copre tutti gli asset rientranti della copertura assicurativa?	Xsi ☐no
	Q.35	[Anti-Malware] - L'organizzazione pianifica ed esegue scansioni periodiche su tutti gli asset informatici che sono oggetto della copertura assicurativa?	X si ☐no
	Q.36	[Anti-Malware] - Le impostazioni del software antivirus / Anti-Malware sono impostate per scansionare anche gli allegati di posta e il contenuto delle pen drive quando utilizzate?	X si ☐no
	Q.37	[Backup] – Con quale frequenza è eseguito il back up dei dati?	Giornalmente
	Q.38	[Backup] Quale modalità di salvataggio e recupero dati fa parte della strategia di back up scelta dall'organizzazione?	☐back up completo ☐back up differenziale Xback up incrementale
	Q.39	[Backup] - L'organizzazione si è dotata di una procedura di backup che identifica le informazioni critiche per il business?	X si ☐no
	Q.40	[Backup] - Dove sono salvate le copie di back up?	X supporti esterni (Server o NAS, chiavette USB, dischi esterni, etc.) ☐Cloud
	Q.41	[Backup] – Le copie di back up salvate su supporti esterni, sono conservate in siti alternativi / secondari per garantire l'efficacia dei processi di Disaster Recovery?	X si ☐no
	Q.42	[Backup] - Vengono eseguiti periodicamente test di ripristino, in particolare dei database che sono oggetto	☐si Xno

		della copertura assicurativa?	
	Q.43	[Backup] - Le copie di backup vengono protette in base al livello di confidenzialità delle informazioni che contengono?	X si ☐no
	Q.44	[Backup]- Vengono eseguiti i backup delle configurazioni degli apparati di rete (es. router, firewall ecc.)?	X si ☐no
	Q.45	[Raccolta Log & Monitoraggio] - L'organizzazione 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"?	X si ☐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)?	X si ☐no
	Q.47	[Raccolta Log & Monitoraggio] - L'organizzazione si è dotata di sistema di correlazione e gestione dei log che supporta le funzioni interne / security nell'identificazione e nell'analisi degli eventi ritenuti critici, anche in ottica forense?	X si ☐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?	X si ☐no
	Q.49	[Raccolta Log & Monitoraggio] – L'organizzazione si è dotata di un sistema di Log Management in grado di monitorare gli accessi eseguiti dagli amministratori e dagli operatori di sistema sui sistemi aziendali?	X si ☐no
	Q.50	[Raccolta Log & Monitoraggio] – Quali misure di protezione sono state adottate dall'organizzazione 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 X Altro, specificare: Funzionalità insita nel software di collezionamento
	Q.51	[Raccolta Log & Monitoraggio] – Indicare le tempistiche di conservazione dei file di log stabilite dall'organizzazione.	☐< 6 mesi ☐≥ 6 mesi ☐≥ 12 mesi X Altro, specificare: secondo disposizioni di legge
	Q.52	Sono attuate procedure per controllare l'installazione di software sui sistemi gestiti?	X si ☐no
	Q.53	[Gestione vulnerabilità tecniche] – L'organizzazione effettua, su tutti gli asset rientranti nel perimetro, dei test di sicurezza periodici (es. Vulnerability Assessment, penetration test) e attività di Risk Analysis?	X si ☐no In caso affermativo, descrivere le principali criticità emerse Generalmente sono state rilevate problematiche sull'aggiornamento di componenti software o errori nel software che sono stati prontamente rimediati

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

F	**Q.60**	L'organizzazione si è dotata di un sistema di selezione dei	☐si Xno

ORNITORI ESTERNI		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?	
	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 ?	X si ☐no
	Q.62	I fornitori di servizi cloud sono in possesso di certificazioni professionali (esempio CCSP Certified Cloud Security Professional, EXIN Cloud Computing Foundation, EC Council CAST 618 Designing and Implementing Cloud Security, ecc.)?	X si ☐no

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

CONTINUI	**Q.66**	L'organizzazione ha implementato un processo documentato di Business Impact Analysis (BIA) regolarmente aggiornato che identifichi gli impatti in termini di tempi di interruzione, danni (es. patrimoniali diretti e indiretti) e relativi tempi di ripristino?	Xsi ☐no
	Q.67	L'organizzazione si è dotata di un piano di ripristino o	X si ☐no

TA' OPERATIVA		Business Continuity Plan (BCP) integrato con procedure operative e istruzioni di ripristino dettagliate?	
	Q.68	L'organizzazione identifica e definisce in un Disaster recovery Plan tutte le attività di ripristino tecnico?	☐si Xno
	Q.69	Sono testati regolarmente:	X il piano di business continuity X il piano di disaster recovery
	Q.70	L'organizzazione ha adottato di una procedura 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?	X si ☐no
	Q.71	Si coinvolgono i fornitori nei test di continuità operativa?	Xsi ☐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 dell'organizzazione:	
		Attività (o settori)	*Massimo periodo di interruzione prima di avere un impatto negativo*
		Tutti i settori	☐Immediatamente X>4ore ☐>12ore ☐>24ore ☐>48 ore ☐>5giorni ☐mai
			☐Immediatamente ☐>4ore ☐>12ore ☐>24ore ☐>48 ore ☐>5giorni ☐mai
			☐Immediatamente ☐>4ore ☐>12ore ☐>24ore ☐>48 ore ☐>5giorni ☐mai
			☐Immediatamente ☐>4ore ☐>12ore ☐>24ore ☐>48 ore ☐>5giorni ☐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'organizzazione ha implementato un processo di Incident Management/Response (persone, ruoli, responsabilità)?	Xsi ☐no
	Q.75	Esistono playbook (elenchi azioni predefinite) in funzione del tipo di incidente occorso (es. sospensione cautelativa del sistema colpito, cambio password, ecc.)?	☐si Xno

Sez.3

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'organizzazione?	
		Tipologia dei dati trattati	*Volume dei dati trattati*
		☐dati finanziari (carte di credito/ debito/conto corrente)	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000
		Xdati personali di terzi Soggetti	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000
		X Informazioni sanitarie	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000
		☐proprietà intellettuale/copyrights/segreti commerciali	☐≤100 ☐≤1.000 ☐≤100.000 ☐≤1.000.000 ☐≥1.000.000
	Q.77	L'organizzazione 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 (es. prevedendo delle informative conformi da rendere prima di raccogliere i dati), raccolta del consenso informato prima di procedere a determinati trattamenti (es. marketing), etc.*	Xsi ☐no
	Q.78	Indicare le misure organizzative implementate per l'adeguamento alla normativa nazionale ed europea in materia di trattamento dei dati	X aggiornamento informative (dipendenti, clienti, sito internet - inclusa Cookie Policy, ecc.) X periodiche sessioni di formazione per dipendenti in materia privacy X processo di raccolta e gestione di consensi informati X tutele rafforzate nel trattamento di categorie particolari di dati (es. informazioni sanitarie) X redazione e aggiornamento registro dei trattamenti X aggiornamento nomine per il trattamento dei dati (incaricati al trattamento, responsabili, amministratori di sistema, etc.) ☐ trasferimento dati extra UE nel rispetto delle condizioni dalla normativa (art. 44, 45 e 46 GDPR) ☐Altro _____
	Q.79	Quali delle seguenti Policy (nelle quali sono anche definiti ruoli e responsabilità) sono state adottate dall'organizzazione?	X Data Breach ☐ Data Retention (nella quale sono stati stabiliti i termini di conservazione e relativa cancellazione dei dati per tutti i trattamenti) X Gestione delle richieste degli interessati in materia privacy XRegolamento sul corretto utilizzo dei sistemi informatici aziendali ☐Altro, specificare _____
	Q.80	A chi è attribuita l'attività di gestione della privacy dell'organizzazione?	☐Società di consulenza o studio legale X Ufficio privacy all'interno dell'azienda (Privacy manager) ☐Libero professionista
	Q.81	L'organizzazione ha nominato un Responsabile della protezione dei dati (DPO)?	X si ☐no ☐non soggetta
	Q.82	L'organizzazione effettua i seguenti trattamenti:	☐ Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive (es. screening dei propri clienti utilizzando database di rischio creditizio/lotta alle frodi/riciclaggio e finanziamento del terrorismo (AML/CTF), creazione di profili comportamentali /marketing a partire dalla navigazione sul proprio sito, etc.) ☐ Decisioni automatizzate che producono significativi effetti giuridici sull'interessato (es. selezione candidati tramite algoritmo) ☐ Utilizzo nuove soluzioni tecnologiche e organizzative (es. associazione di tecniche dattiloscopiche e riconoscimento del volto per il controllo degli accessi fisici) ☐ Monitoraggio regolare e sistematico (es. 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 (es. mobile payment).
	Q.83	Sono previsti dei sistemi dai quali può derivare un controllo anche a distanza dei dipendenti?	☐si X no In caso affermativo, indicare quali: ☐sistemi di geolocalizzazione (veicoli) ☐videosorveglianza ☐monitoraggio della navigazione internet (sistema di log, etc.) ☐altro_____
	Q.84	Nel caso in cui l'organizzazione 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?	X si ☐no

Sez.4

CONTENUTI MULTIMEDIALI

GESTIONE DELLA MULTIMEDIALITA'	**Q.85**	Di quale tipologia di canali digitali si avvale l'organizzazione?	x 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 (es. in fase di iscrizione al sito, newsletter, etc.) ☐ procedure di opt out, compreso l'inserimento del link per la disiscrizione al servizio (es. newsletter) ☐ procedure per la tracciabilità e/o profilazione degli utenti/ visitatori (es. cookie, etc.)
	Q.87	L'organizzazione 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) _____ x no, la pubblicità viene gestita da un ufficio interno all'organizzazione
	Q.88	L'organizzazione 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?	x si ☐no Social Media Policy - potere di controllo e rimozione di contenuti
	Q.89	La vagliatura dei contenuti pubblicati sui canali online dell'organizzazione, comprende:	x violazione del diritto alla riservatezza x violazione del copyright x lesione dell'altrui reputazione ☐altro, specificare_____
	Q.90	L'organizzazione dispone di una procedura per rispondere ad eventuali reclami sui contenuti creati e pubblicati, considerati calunniosi, illegali o in violazione al diritto alla privacy di terzi?	x si ☐no I reclami sono gestiti secondo istruzione operativa interna

DICHIARAZIONI	
	La firma del presente questionario non obbliga il proponente all'acquisto delle polizza
	Il sottoscritto, in forza dei poteri di sottoscrizione e di rappresentanza disgiunta della società, qui di seguito 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.