



Fascicolo 2.14\2021\3

Pagina 1

FAQ 9 - 12

Oggetto: : Procedura aperta per l'affidamento dei servizi assicurativi del Comune di Arese - LOTTO 1) RESPONSABILITA' CIVILE VERSO TERZI E PRESTATORI DI LAVORO (RCT/O) – CIG 8769912852; LOTTO 2) RC PATRIMONIALE – CIG 876992965A; LOTTO 3) TUTELA LEGALE – CIG 87699442BC; LOTTO 4) CYBER RISKS – CIG 8769955BCD; ; LOTTO 5) ALL RISKS PROPERTY – CIG 87699610C4; LOTTO 6) INFORTUNI – CIG 8769968689; LOTTO 7) R.C. AUTO LIBRO MATRICOLA E CVT – CIG 8769973AA8

QUESITO 9

Oggetto: QUESTIONARIO CYBER RISK

Con la presente, avremmo necessità della compilazione di nostro questionario allegato, al fine di poter acquisire ulteriori informazioni utili allo studio del lotto Cyber Risk.

1	1. Per quanto riguarda le attività messe in campo dal Richiedente per mitigare il phishing, selezionare tutte le risposte pertinenti	RISPOSTA
	Il Richiedente eroga, almeno una volta all'anno, ai dipendenti formazione sulla "consapevolezza della sicurezza informatica"	
	Il Richiedente , almeno una volta all'anno, utilizza attacchi di phishing simulati per testare la consapevolezza della sicurezza informatica dei dipendenti	
	Qualora il Richiedente conduca attacchi di phishing simulati, la percentuale di successo nell'ultimo test è stata inferiore al 15% (meno del 15% dei dipendenti è stato "indotto in errore" con successo)	
	Il Richiedente "contrassegna", o comunque evidenzia in altro modo, tutte le e-mail provenienti dall'esterno dell'organizzazione.	X
	Il Richiedente ha un processo per segnalare e-mail sospette a un team di sicurezza interno che ha il compito di indagare	X



	Nessuno dei precedenti.	
	Commento aggiuntivo sugli sforzi per mitigare il phishing:	
2	Il Richiedente dispone di un processo documentato per rispondere alle campagne di phishing (mirate specificamente al Richiedente o meno)?	
	Si	
	No	X
	Se "Sì", descrivere i passaggi principali della risposta	
3	Per quanto riguarda le attività/presidi di sicurezza adottati dal Richiedente per bloccare siti web e / o email potenzialmente dannose, <u>selezionare tutte le risposte pertinenti:</u>	
	Il Richiedente utilizza una soluzione di filtraggio della posta elettronica che blocca allegati dannosi noti e tipi di file sospetti, inclusi gli eseguibili	X
	Il Richiedente utilizza una soluzione di filtro della posta elettronica che blocca i messaggi sospetti in base al contenuto o agli attributi del mittente	X
	Il Richiedente utilizza una soluzione di filtraggio web che impedisce ai dipendenti di visitare pagine web dannose o sospette note	X
	Il Richiedente utilizza blocchi verso domini non categorizzati e/o di nuova registrazione utilizzando proxy Web o filtri DNS	X
	Il Richiedente utilizza una soluzione di filtro web che blocca i download noti come dannosi o sospetti, inclusi gli eseguibili	X

	La soluzione di filtraggio della posta elettronica del Richiedente ha la capacità di eseguire allegati sospetti in una sandbox	
	Le funzionalità di filtro web del Richiedente sono efficaci su tutte le risorse aziendali, anche se la risorsa aziendale non si trova su una rete aziendale (ad esempio, le risorse sono configurate per utilizzare filtri web basati su cloud o richiedono una connessione VPN per navigare in Internet).	
	Nessuno dei precedenti	
	Commenti aggiuntivi attività/presidi di sicurezza adottati dal Richiedente per bloccare siti Web e / o e-mail dannose	
4	Per quanto riguarda l'autenticazione per i dipendenti che accedono da remoto alla rete aziendale e a qualsiasi servizio basato su cloud in cui possono risiedere dati sensibili (incluso l'accesso alla VPN, la posta elettronica e i CRM basati su cloud; definiti come "accesso remoto alle risorse aziendali), selezionare la descrizione che meglio riflette la postura del Richiedente [nota: nel presente documento, "autenticazione a più fattori" – MFA - significa un'autenticazione che utilizzi almeno due diversi tipi di possibili fattori di autenticazione (qualcosa che sai, qualcosa hai e qualcosa che sei); il Richiedente può fornire ulteriori spiegazioni di seguito]	
	L'accesso remoto alle risorse aziendali richiede un nome utente e una password validi (autenticazione a fattore singolo)	X
	L'autenticazione a più fattori è attiva per alcuni tipi di accesso remoto alle risorse aziendali, ma non tutti	
	L'autenticazione a più fattori è richiesta dalla politica per tutti gli accessi remoti alle risorse aziendali; tutte le eccezioni alla politica sono documentate	



	Il Richiedente non fornisce l'accesso remoto ai dipendenti	
	Commento aggiuntivo sull'autenticazione per i dipendenti:	
5	Per quanto riguarda l'autenticazione per appaltatori e fornitori indipendenti che accedono in remoto alla rete aziendale e a qualsiasi servizio basato su cloud in cui i dati sensibili possono risiedere (compreso l'accesso VPN, e-mail e CRM basati su cloud; tutti insieme definiti come "accesso remoto alle risorse aziendali"), selezionare la descrizione che meglio riflette la posizione del Richiedente : (Il Richiedente può fornire ulteriori spiegazioni di seguito)	
	L'accesso remoto alle risorse aziendali richiede un nome utente e una password validi (autenticazione a fattore singolo)	X
	L'autenticazione a più fattori è attiva per alcuni tipi di accesso remoto alle risorse aziendali, ma non tutti.	
	L'autenticazione a più fattori è richiesta dalla politica per tutti gli accessi remoti alle risorse aziendali; tutte le eccezioni alla politica sono documentate.	
	Il Richiedente non fornisce l'accesso remoto a contraenti / fornitori indipendenti	
	Commento aggiuntivo sull'autenticazione per appaltatori / fornitori indipendenti:	
6	L'implementazione dell'autenticazione a più fattori del Richiedente soddisfa anche il criterio secondo cui la compromissione di un singolo dispositivo comprometterà solo un singolo autenticatore?(Ad esempio: se l'autenticazione richiede una password (conoscenza) e un token (possesso), di per se stesso il criterio di cui sopra non sarebbe soddisfatto là dove il token per dimostrare il possesso sia mantenuto sul medesimo dispositivo che conserva anche la	



	password, esponendoli entrambi i fattori se il dispositivo fosse compromesso)	
	Non applicabile (il Richiedente non utilizza l'autenticazione a più fattori)	X
	No; L'implementazione multifattoriale del Richiedente non soddisfa i criteri di cui sopra.	
	Sì; l'implementazione multifattoriale del Richiedente soddisfa i criteri di cui sopra.	
	Commento aggiuntivo sull'implementazione dell'autenticazione a più fattori:	
7	Per quanto riguarda la sicurezza degli endpoint e delle workstation (desktop e laptop) del Richiedente , <u>selezionare tutte le risposte pertinenti</u> :	
	La politica del Richiedente è che tutte le workstation siano dotate di antivirus con funzionalità euristiche (non basate solo su firma)	X
	Il Richiedente utilizza strumenti di sicurezza degli endpoint con funzionalità di rilevamento del comportamento e mitigazione degli exploit.	X
	Il Richiedente dispone di un gruppo interno che monitora l'output degli strumenti di sicurezza degli endpoint e indaga su eventuali anomalie.	X
	Nessuno dei precedenti.	
	Commento aggiuntivo sulle funzionalità di sicurezza degli endpoint:	

8	Per quanto riguarda il monitoraggio delle log (segnalazioni) degli strumenti di sicurezza, selezionare la descrizione che meglio riflette la capacità di gestione del Richiedente :	
	Il Richiedente non dispone di personale dedicato al monitoraggio delle operazioni di sicurezza (un "Centro operativo di sicurezza – c.d. SOC: Security Operations Center ")	X
	Il Richiedente ha un Security Operations Center, ma non è attivo 24 ore su 24, 7 giorni su 7 (può essere interno o esterno)	
	Il Richiedente ha un monitoraggio 24 ore su 24, 7 giorni su 7 delle operazioni di sicurezza da parte di una terza parte (es. un Fornitore di Servizi di Sicurezza Gestiti c.d. Managed Security Services Provider)	
	Il Richiedente ha un monitoraggio interno 24 ore su 24, 7 giorni su 7 delle operazioni di sicurezza	
	Commento aggiuntivo sul monitoraggio della sicurezza:	
9	Qual è stato il tempo medio necessario al Richiedente per valutare e contenere gli incidenti di sicurezza delle workstation dall'inizio dell'anno?	
	Il Richiedente non tiene traccia di questa metrica / Non lo so	
	meno di 30 minuti	
	30 minuti-2 ore	
	2-8 ore	X



	Più di 8 ore	
	Commento aggiuntivo sul tempo medio per rimediare:	
10	Per quanto riguarda i controlli di accesso per la postazione di lavoro di ogni utente, selezionare la descrizione che meglio riflette la postura del Richiedente (Il Richiedente può fornire ulteriori spiegazioni di seguito):	
	Nessun dipendente è nel gruppo degli amministratori o ha accesso come amministratore locale alla propria workstation	
	La politica del Richiedente prevede che i dipendenti per impostazione predefinita non siano nel gruppo degli amministratori e non abbiano accesso amministrativo locale; tutte le eccezioni alla politica sono documentate	X
	Alcuni dipendenti del Richiedente fanno parte del gruppo degli amministratori o sono amministratori locali	
	Non lo so	
	Commento aggiuntivo sui controlli di accesso per le workstation:	
11	Per quanto riguarda la protezione delle credenziali privilegiate, <u>selezionare tutto ciò che si applica rispetto alla postura del Richiedente</u>	
	Gli amministratori di sistema del Richiedente dispongono di una credenziale unica e privilegiata per le attività amministrative (separata dalle credenziali utente per l'accesso quotidiano, e-mail, ecc.)	X



	Gli account privilegiati (inclusi gli amministratori di dominio) richiedono l'autenticazione a più fattori	
	Gli account privilegiati sono conservati in una cassaforte per password che richiede all'utente di "estrarre" le credenziali (che vengono ruotate in seguito)	X
	È disponibile un registro di tutti gli utilizzi degli account privilegiati per almeno gli ultimi trenta giorni	
	Le workstation ad accesso privilegiato (workstation che non hanno accesso a Internet o alla posta elettronica) vengono utilizzate per l'amministrazione di sistemi critici (inclusi server di autenticazione /Controller di dominio)	
	Nessuno dei precedenti	
	Commento aggiuntivo sulla protezione delle credenziali privilegiate:	
12	Fornire dettagli sull'utilizzo da parte del Richiedente di Microsoft Active Directory (in tutti i domini / foreste):	
	Il Richiedente non utilizza Microsoft Active Directory (indicare a destra)	
	Numero di account utente nel gruppo del Dominio Amministratori (inclusi gli account di servizio, se presenti, in questo totale)	138
	Numero di account di servizio nel gruppo del Dominio Amministratori: ("account di servizio " <u>indica un account utente creato appositamente per un'applicazione o un servizio per interagire con altri computer appartenenti a un dominio</u>):	4
	Commento aggiuntivi sul numero degli amministratori di dominio	



13	<p>Quanti utenti hanno account con privilegi permanenti per gli endpoint (server e workstation)?</p> <p>(Ai fini di questa domanda, "account con privilegi" <u>indica i diritti per configurare, gestire e supportare in altro modo questi endpoint; gli utenti che devono "effettuare il check-out" delle credenziali non dovrebbero essere inclusi. Il Richiedente può fornire ulteriori spiegazioni di seguito</u>)</p>	
	Inserisci un numero intero	2
	Commento aggiuntivo sul numero di account con privilegi	
	UTENTI CHE POSSEGGONO I DIRITTI DI AMMINISTRATORI DI DOMINIO SONO: PERSONALE DEL CED (OLTRE AGLI UTENTI DI SERVIZIO UTILIZZATI PER APPLICATIVI)	
14	<p>Per quanto riguarda la sicurezza dei sistemi esposti verso l'esterno, <u>selezionare tutto ciò che si applica alla postura del Richiedente</u></p>	
	Il Richiedente esegue un test di penetrazione almeno una volta all'anno per valutare la sicurezza dei suoi sistemi rivolti verso l'esterno	
	Il Richiedente ha un Web Application Firewall (WAF) davanti a tutte le applicazioni rivolte all'esterno ed è in modalità di blocco	
	Il Richiedente utilizza un servizio esterno per monitorare la sua superficie di attacco (sistemi esterni / rivolti a Internet)	
	Nessuno dei precedenti	X
15	Qual è il tempo target del Richiedente per distribuire le patch "critiche" intendendosi quelle di massima priorità (come determinata dagli standard del	



	Richiedente per la distribuzione delle patch)?	
	Non esiste una politica definita per la distribuzione delle patch.	
	Entro 24 ore	
	24-72 ore	
	3-7 giorni	X
	> 7 giorni	
	Commento aggiuntivo sui tempi target per l'applicazione delle patch	
16	Qual è stata il livello di conformità da inizio anno del Richiedente ai propri standard per la distribuzione di patch critiche? (Il Richiedente può fornire ulteriori spiegazioni di seguito)	
	Il Richiedente non tiene traccia di questa metrica / Non lo so	
	>95%	
	90-95%	X
	80-90%	
	<80%	



	<p>Commento aggiuntivo sulla conformità delle patch:</p>	
17	<p>Per quanto riguarda le capacità di monitoraggio della rete del Richiedente, <u>selezionare tutte le risposte pertinenti:</u></p>	
	<p>Il Richiedente utilizza uno strumento SIEM (Security Information and Event Monitoring) per correlare l'output di più strumenti di sicurezza</p>	X
	<p>Il Richiedente monitora il traffico di rete per trasferimenti di dati anomali e potenzialmente sospetti</p>	
	<p>Il Richiedente monitora i problemi di prestazioni e capacità di archiviazione (come utilizzo elevato della memoria o del processore o assenza di spazio libero su disco).</p>	
	<p>Il Richiedente dispone di strumenti per monitorare la perdita di dati (DLP) e sono in modalità di blocco.</p>	
	<p>Nessuno dei precedenti</p>	
	<p>Commento aggiuntivo sul monitoraggio della rete:</p>	
18	<p>Relativamente alla limitazione dei movimenti laterale, <u>selezionare tutto ciò che si applica alla postura del Richiedente</u> (Il Richiedente può fornire ulteriori spiegazioni di seguito):</p>	
	<p>Il Richiedente ha segmentato la rete in base all'area geografica (e.g.: il traffico tra uffici in luoghi diversi è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale)</p>	



	Il Richiedente ha segmentato la rete in base alla funzione aziendale (ad esempio il traffico tra asset che supportano funzioni diverse, ad esempio HR e Finance, è negato a meno che non sia richiesto per supportare uno specifico requisito aziendale	X
	Il Richiedente ha implementato regole del firewall host che impediscono l'uso di Remote Desktop Protocol - RDP per accedere alle workstation	
	Il Richiedente ha configurato tutti gli account di servizio per negare gli accessi interattivi	X
	Nessuno dei precedenti	
	Commento aggiuntivo sulla segmentazione:	
19	Immettere la data dell'ultima esercitazione su ransomware da parte del Richiedente ovvero selezionare l'apposita casella se non ne è stata eseguita nessuna esercitazione	
	Data:	
	Non è stata condotta alcuna esercitazione su ransomware	X
20	Il Richiedente dispone di un piano documentato per rispondere al ransomware di un fornitore / fornitore di terze parti o cliente? In caso affermativo, indicare i passaggi principali	
	No	X
	Sì	



	Fasi principali della risposta al ransomware di terze parti:	
21	Per quanto riguarda la verifica dell'efficacia dei controlli di sicurezza, <u>selezionare tutto ciò che si applica al Richiedente</u> (Il Richiedente può fornire ulteriori spiegazioni di seguito)	
	Il Richiedente utilizza software BAS (Breach and Attack Simulation) per verificare l'efficacia dei controlli di sicurezza	
	Il Richiedente dispone di un "red team" interno che verifica i controlli di sicurezza e la risposta	
	Nell'ultimo anno Il Richiedente ha incaricato un fornitore esterno di simulare gli attori delle minacce e testare i controlli di sicurezza	
	Nessuno dei precedenti	X
	Commento aggiuntivo sulla verifica dei controlli:	
22	Per quanto riguarda le funzionalità di ripristino di emergenza, <u>selezionare tutto ciò che si applica al Richiedente:</u>	
	Esiste un processo per la creazione di backup, ma non è documentato e/o ad hoc	
	Il Richiedente dispone di una politica di ripristino di emergenza documentata, inclusi standard per i backup basati sulla criticità delle informazioni	
	Almeno due volte all'anno, il Richiedente verifica la propria capacità di	



	ripristinare tempestivamente diversi sistemi e dati critici dai propri backup	
	Nessuno dei precedenti	X
23	Qual è l'RTO (Recovery Time Objective) del Richiedente per i sistemi critici?	
	Il Richiedente non ha un RTO / Non lo sa	X
	< 4 ore	
	4-24 ore	
	1 to 2 giorni	
	2-7 giorni	
24	Per quanto riguarda le capacità di backup, <u>selezionare tutto ciò che si applica al Richiedente:</u>	
	La strategia di backup del Richiedente include backup offline (possono essere archiviati in sede)	X
	La strategia di backup del Richiedente include backup offline archiviati fuori sede	X
	È possibile accedere ai backup del Richiedente solo tramite un meccanismo di autenticazione esterno alla nostra Active Directory aziendale	
	Commento aggiuntivo sulle funzionalità di backup:	

25	Il Richiedente dispone di una politica in base alla quale tutti i dispositivi portatili utilizzano la crittografia completa del disco?	
	Sì	
	No	X
	Commento aggiuntivo:	

QUESITO 10

Oggetto: Chiarimenti

Testo: in relazione al lotto 5 All Risks chiediamo quanto di seguito riportato (**N.B. La numerazione delle domande è inserita dalla Stazione appaltante**): (1) Con la presente siamo a richiedere che per il rischio Cyber venga inserita la seguente formulazione in merito alla relativa esclusione: “Si intendono esclusi i danni di qualsiasi natura, diretti o indiretti, derivanti da cancellazione di dati, mancato, errato, inadeguato funzionamento del sistema informatico e/o di qualsiasi macchinario, impianto, apparecchiatura, componente elettronica, firmware, software e hardware in ordine alla gestione del tempo (ore e date) oppure in seguito ad attacco od infezione di virus informatici nonché conseguenti ad operazioni di download, installazione e/o modifica di programmi.” (2) chiediamo cortese conferma che la garanzia property escluda la fattispecie così come sotto definita: **ESCLUSIONE DELLE MALATTIE TRASMISSIBILI**: La presente polizza non copre qualsiasi perdita, danno, responsabilità, richiesta di risarcimento di danni, costo o spesa, causata, dovuta a, risultante o derivante da, ad una malattia trasmissibile o al timore o minaccia (reale o presunta) di una malattia trasmissibile, nonché i danni, diretti, indiretti e/o conseguenti che derivino dagli atti e dalle misure per prevenire il contagio disposte delle competenti Autorità, anche in relazione alla chiusura e alla restrizione dell’attività o per finalità di decontaminazione e disinfezione. Per “malattia trasmissibile” si intende qualsiasi malattia che può essere trasmessa per mezzo di qualsiasi sostanza o agente, da qualsiasi organismo ad un altro, dove: 2.1. il termine sostanza o agente include, a titolo esemplificativo ma non esaustivo, un virus, un batterio, un parassita un altro organismo o qualsiasi variazione di esso, sia esso considerato vivente o meno; 2.2. il metodo di trasmissione diretto o indiretto include, a titolo esemplificativo ma non esaustivo,

la trasmissione per via aerea, la trasmissione di fluidi corporei, la trasmissione da o verso qualsiasi superficie o oggetto, solido, liquido o gas oppure tra organismi 2.3. la malattia, la sostanza o l'agente può causare o minacciare di causare danni alla salute o al benessere umano oppure può minacciare di causare danni, deterioramenti, perdita di valore o di commerciabilità o perdita di uso della proprietà. (3) Siamo a chiedere se vi è disponibilità da parte dell'Ente, in caso di aggiudicazione, a consentire l'inserimento, nei Capitolati ove non prevista, della seguente Clausola: "ESCLUSIONE OFAC (Sanctions Limitations Exclusion Clause) Gli [Assicuratori] [Riassicuratori] non sono tenuti a fornire alcuna copertura o a disporre alcun risarcimento ai sensi del presente contratto, qualora ciò implichi qualsiasi tipo di violazione di legge o regolamento in materia di sanzioni internazionali, che esponga gli [Assicuratori] [Riassicuratori], la loro capogruppo o la loro controllante a qualsiasi violazione delle leggi e dei regolamenti in materia di sanzioni internazionali.?" (4) In relazione alla statistica Sinistri allegata chiediamo dettagli in relazione al sinistro di maggior portata, chiediamo inoltre se i sinistri elencati senza importo e status siano da intendersi senza seguito e definitivamente chiusi.

RISPOSTA

Punti nn. (1) – (2) - (3): si segnala che non sarà possibile apportare modifiche al capitolato tecnico proposto in gara, pertanto l'esclusione dei rischi Cyber resterà prevista nei termini espressi nel capitolato stesso mentre "esclusione malattie trasmissibili" e "esclusione OFAC", entrambe non pertinenti per il rischio assicurato, non saranno espressamente previste. Per la clausola cd. "esclusione OFAC" si rinvia anche alla FAQ n. 5 pubblicata in data 16.06.2021.

Punto n. (4): facendo riferimento al Lotto n. 5 All Risks richiamato in principio nel quesito, relativamente al sinistro n. 809200, liquidato per € 100.000,00, si specifica che trattasi di cedimento strutturale della parte storica dell'edificio sede del Comune di Arese (lato edificio fronteggiante Piazza Carlo Alberto Dalla Chiesa, angolo via Roma). Il sinistro è chiuso, pagato.

Le posizioni che risultano senza riserva e senza importo liquidato son da intendersi chiusi senza seguito.

QUESITO 11

Oggetto: RICHIESTA INFORMAZIONI

Testo: Con la presente, si chiedono le seguenti informazioni (**N.B. La numerazione delle domande è inserita dalla Stazione appaltante**): **(1)** - se il Comune abbia la proprietà o gestisca, direttamente o indirettamente, case di riposo, RSA o strutture similari; **(2)** - quali siano le attività socioassistenziali di cui si occupa il Comune; **(3)** - se gli importi liquidati siano al lordo o al netto della franchigia contrattuale e **(4)** quale sia la franchigia in corso negli anni cui la statistica sinistri si riferisce.

RISPOSTA

Punto n. (1): richiamata la FAQ n. 6 pubblicata in data 16.06.2021, si riscontra come segue:

è presente una RSA, gestita con affidamento in house all'Azienda Speciale denominata "Casa di Riposo – Gallazzi Vismara", ente strumentale del Comune di Arese dotato di personalità giuridica e autonomia patrimoniale (vd. DUP, pag. 51 e pagg. 53 ss.); inoltre è presente un servizio, di natura socio-sanitaria, consistente in una Comunità Alloggio per persone disabili ("La Cometa"), con affidamento in house all'Azienda Consortile Ser.Co.p. (vd. punto successivo);

Punto n. (2): per la panoramica delle attività socio-assistenziali di cui si occupa il Comune è possibile consultare il Documento Unico di Programmazione 2021/2023 del Comune di Arese (in particolare, pagg. 51 e ss.), disponibile presso il sito dell'Ente al link: https://www.comune.arese.mi.it/Articoli/Amministrazione-Trasparente/Amministrazione-Trasparente/310-6727%5E2021.asp?ID=6727&ID_MacroMenu=8

Il Comune di Arese gestisce molte attività socio-assistenziali tramite l'Azienda Speciale Consortile Ser.Co.P. (Consorzio Servizi comunali alla Persona), ente strumentale istituito da diversi Comuni per l'esercizio di funzioni socio-assistenziali, socio-educative e socio-sanitarie integrate e, più in generale, per la gestione dei servizi alla persona a prevalente carattere sociale, in relazione alle competenze istituzionali degli Enti consorziati (vd. DUP, pagg. 59 ss.).

Alcuni servizi socio-assistenziali (specificamente: servizio di integrazione scolastica; servizio dei centri ricreativi diurni – cd. centri estivi; servizio pasti domiciliari per anziani/disabili; servizio di trasporti sociali per anziani/disabili) sono gestiti direttamente dal Comune, con affidamento in appalto o tramite convenzionamento con associazioni di volontariato.

Punto n. (3): vd. FAQ n. 1 pubblicata in data 16.06.2021;

Punto n. (4): il documento Allegato 10 al Progetto fornisce le informazioni relative alle polizze in corso, tra cui le franchigie ove previste, per il medesimo periodo cui si riferiscono le statistiche sinistri (dal 31.12.2015 ad oggi).

QUESITO 12

Oggetto: SOGGETTI AMMESSI ALLA PARTECIPAZIONE ALLA GARA

Testo: A) Esecuzione negli ultimi tre anni di servizi analoghi Gli operatori economici devono aver eseguito con buon esito nell'ultimo triennio antecedente la data di pubblicazione della presente procedura, in favore di destinatari pubblici e/ o privati, servizi relativi a rischi analoghi a quelli della tipologia di Lotto al quale intendono partecipare, con premio (al lordo delle eventuali imposte governative) complessivo minimo/non inferiore alla base di gara del Lotto in questione, ovvero: I. per il Lotto n. 1, nel relativo ramo (RC Generale): Euro 344.000,00; RISPETTO ALL'ARTICOLO CITATO, SI INTENDE CHE LA SOMMA DEI SERVIZI ESEGUITI NEGLI ULTIMI TRE ANNI SIA IN FAVORE DI DESTINATARI PUBBLICI SIA IN FAVORE DI DESTINATARI PRIVATI DEBBA ESSERE NON INFERIORE O UGUALE A QUELLO DEL LOTTO IN QUESTIONE?

RISPOSTA

Si conferma. Si precisa che i destinatari dei servizi analoghi svolti nel triennio devono essere pubbliche amministrazioni o soggetti di diritto pubblico (destinatari pubblici) e/o persone giuridiche di diritto privato (destinatari privati). Sono esclusi i servizi svolti a favore di persone fisiche.

Distinti saluti

Il RUP Arese
Dott.ssa R. Paganini

Il RUP SUA
Avv. P. Trapani