OGGETTO: GARA A PROCEDURA APERTA PER L'ACQUISIZIONE DI SERVIZI DI BANCHE DATI PER LA VIGILANZA ISPETTIVA PER INAIL– ID 2914

I chiarimenti della gara sono visibili sui siti: www.consip.it; www.acquistinretepa.it; www.mef.it

***

1) Domanda

1. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 9 a pag. 25 nel seguente modo: "*Nel caso in cui per le prestazioni del Contratto che comportano il trattamento di dati personali il Fornitore/ Responsabile ricorra a subappaltatori o subcontraenti è obbligato a nominare tali operatori a loro volta sub-Responsabili del trattamento sulla base della modalità sopra indicata e comunicare l'avvenuta nomina al titolare.*
   Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale del trattamento assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE. In caso di mancato adempimento da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti ***entro le soglie stabilite nella polizza assicurativa (CYBER RISK)****; la Committente potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi* ***nei limiti di 4 ore e massimo una volta all'anno****. Nel caso in cui tali garanzie risultassero insussistenti o inidonee la Committente potrà risolvere il contratto con il Responsabile iniziale.*
2. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 11 a pag. 25/26 nel seguente modo: "*Il Responsabile del trattamento manleverà e terrà indenne il Titolare da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub-fornitori* ***entro le soglie stabilite nella polizza assicurativa (CYBER RISK)****."*
3. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 14 a pag. 26 nel seguente modo: "*Il Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali relativamente ai servizi oggetto del presente contratto; inoltre, deve assistere il Titolare nel caso di richieste formulate*

dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto ***salvo diversa indicazione da parte dell'Autorità****."*

4. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 15 a pag. 26 nel seguente modo: "Il *Responsabile del trattamento deve mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche o circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali* ***nei limiti di 4 ore e massimo una volta all'anno; in alternativa tali verifiche potranno essere realizzate mediante idonee attestazioni e certificazioni rilasciate da enti terzi indipendenti sul sistema di gestione per la sicurezza delle informazioni (secondo norma ISO/IEC 27001-27017-27018-27035-27701) ovvero sul sistema di gestione della qualità (ISO 9001)****. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di* ~~*tre*~~ ***dieci*** *giorni lavorativi,* ~~*fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso*~~*; nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, la Committente* ~~*applicherà la penale di cui all'art. 12 S e*~~ *diffiderà il Fornitore ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, la Committente potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.*
5. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 19 a pag. 27 nel seguente modo: "~~*Su richiesta del Titolare*~~*, il Responsabile* ***valuta la possibilità di*** ~~*si impegna ad*~~ *adottare, nel corso dell'esecuzione del Contratto, ulteriori garanzie quali l'applicazione di un codice di condotta approvato o di un meccanismo di certificazione approvato di cui agli articoli 40 e 42 del Regolamento UE, quando verranno emanati. La Committente potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.*
6. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 22 a pag. 27 nel seguente modo: "*Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento* ***nei limiti di 4 ore e massimo una volta all'anno; in alternativa tali verifiche potranno essere realizzate mediante idonee attestazioni e certificazioni rilasciate da enti terzi indipendenti sul sistema di gestione per la sicurezza delle informazioni (secondo norma ISO/IEC 27001-27017-27018-27035-27701) ovvero sul sistema di gestione della qualità (ISO 9001).***
7. Si chiede di modificare l'Art. "V ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 23 a pag. 27 nel seguente modo: "*Nel caso in cui il Fornitore agisca in modo difforme o contrario alle legittime istruzioni del Titolare oppure adotti misure di sicurezza inadeguate*

rispetto al rischio del trattamento risponde del danno causato agli "interessati". In tal caso, la Committente potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno ***entro le soglie stabilite nella polizza assicurativa (CYBER RISK****). Resta inteso che il responsabile del trattamento non potrà essere in alcun modo imputabile per eventuali inadempimenti del Titolare agli obblighi previsti dal Regolamento che comportino risarcimenti dei danni causati o sanzioni amministrative pecuniarie. Le Parti prendono atto, che in caso di responsabilità derivante da una violazione del regolamento GDPR ovvero in caso di richieste di risarcimento a seguito di tali violazioni, saranno applicate le disposizioni previsto dall'art. 82 del GDPR."*

Risposta

Non si conferma. La decisione è rimessa all'Amministrazione contraente in sede di stipula del contratto esecutivo.

2) Domanda

Con riferimento al documento "aK_A_ID_2914_-_Banche_dati_INAIL_-_Contratto_Condizioni_speciali" si richiedono le seguenti modifiche/cancellazioni evidenziate:

1. Si chiede di modificare l'Art. "ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 4 a pag. 23 nel seguente modo: "*Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati comuni (es. dati anagrafici e di contatto ecc..); ii) dati sensibili (dati sanitari, opinioni politiche ecc.); ~~iii) dati giudiziari~~.*
2. Si chiede di modificare l'Art. "ARTICOLO 18 S NOMINA RESPONSABILE TRATTAMENTO DATI PERSONALI" punto 7 a pag. 24 nel seguente modo: "*Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre* ***, se del caso****:*
   - *la pseudonimizzazione e la cifratura dei dati personali;*
   - *la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;*
   - *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;*
   - *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;*
   - *la redazione ~~del Piano di Sicurezza~~* ***di un sistema di gestione della sicurezza delle informazioni*** *e l'implementazione delle relative contromisure, conformemente al principio di privacy by design ex art. 25 GDPR;*
   - *i controlli previsti dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI) del Titolare del trattamento, certificato secondo lo Standard ISO 27001, nel rispetto delle policy definite nel SGSI."*

Risposta
Non si conferma. La decisione è rimessa all'Amministrazione contraente in sede di stipula del contratto esecutivo.

3) Domanda
Con riferimento al documento "aO_A_ID_2914_-_Allegato_Privacy_INAIL" si richiedono le seguenti modifiche/cancellazioni evidenziate:
Si chiede di modificare l'Art. "V. ULTERIORI OBBLIGHI DI GARANZIA DEL FORNITORE" a pag. 7 nel seguente modo: "*Il Fornitore si impegna a:*

1. *mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato* ***nei limiti di 4 ore e massimo una volta all'anno; in alternativa tali verifiche potranno essere realizzate mediante idonee attestazioni e certificazioni rilasciate da enti terzi indipendenti sul sistema di gestione per la sicurezza delle informazioni (secondo norma ISO/IEC 27001-27017-27018-27035-27701) ovvero sul sistema di gestione della qualità (ISO 9001)****.*
   Inoltre il Responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.
2. *Trattare i Dati Personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento dei Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o Nazionale cui è soggetto il Responsabile del trattamento. In Tale caso il Responsabile del trattamento informa il Titolare di tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.*
3. *Il Fornitore si impegna a notificare tempestivamente al Titolare ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai Dati Personali del Titolare salvo il caso in cui tale comunicazione non sia vietata dal provvedimento o dalla legge. 4) In simili circostanze, e in ogni caso conformemente a quanto previsto dal GDPR e dalla normativa applicabile, il Fornitore deve: i) informare il Titolare tempestivamente; ii) collaborare con il Titolare, iii) garantire il trattamento riservato di tali informazioni.*
4. *Fornitore prende atto e riconosce che, nell'eventualità di una violazione delle norme in materia di Trattamento dei Dati Personali nonché delle disposizioni di cui al presente Allegato, oltre all'applicazione delle clausole di risoluzione del contratto e delle penali oltre all'eventuale risarcimento del maggior danno* ***entro le soglie stabilite nella polizza assicurativa (CYBER RISK****), il Titolare avrà la facoltà di ricorrere a provvedimenti cautelari, ingiuntivi e sommari o ad altro rimedio equitativo, allo scopo di interrompere immediatamente, impedire o limitare il trattamento, l'utilizzo o la divulgazione dei Dati Personali.*
5. *Il Fornitore si impegna a tenere indenne il Titolare per qualsiasi responsabilità connessa ad eventuali inadempimenti della normativa GDPR e relativa alla sicurezza informatica da parte del Fornitore* ***entro le soglie stabilite nella polizza assicurativa (CYBER RISK****).*

6. *Il Titolare si impegna a tenere indenne il Fornitore per qualsiasi responsabilità connessa ad eventuali inadempimenti della normativa GDPR e relativa alla sicurezza informatica da parte del Titolare del trattamento* ***entro le soglie stabilite nella polizza assicurativa (CYBER RISK).***
7. ***Resta inteso che il responsabile del trattamento non potrà essere in alcun modo imputabile per eventuali inadempimenti del Titolare agli obblighi previsti dal Regolamento che comportino risarcimenti dei danni causati o sanzioni amministrative pecuniarie***
8. ***Le Parti prendono atto, che in caso di responsabilità derivante da una violazione del regolamento GDPR ovvero in caso di richieste di risarcimento a seguito di tali violazioni, saranno applicate le disposizioni previsto dall'art. 82 del GDPR"***.

Risposta
Non si conferma. La decisione è rimessa all'Amministrazione contraente in sede di stipula del contratto esecutivo.

4) Domanda
Con riferimento al documento "aO_A_ID_2914_-_Allegato_Privacy_INAIL" si richiedono le seguenti modifiche/cancellazioni evidenziate:
Si chiede di modificare l'Art. "**IV.A) Misure di sicurezza**" a pag. 6 nel seguente modo:

1. "*Il Titolare e il Fornitore mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e garantire il rispetto degli obblighi di cui all'art. 32 del GDPR. Tali misure comprendono tra le altre****, se del caso****:*
   a) *la pseudonimizzazione e la cifratura dei Dati Personali;*
   b) *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
   c) *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;*
   d) *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;*
   e) *la redazione ~~del Piano di Sicurezza~~* ***di un sistema di gestione della sicurezza delle informazioni*** *e l'implementazione delle relative contromisure, conformemente al principio di privacy by design ex art. 25 GDPR;*
   f) *i controlli previsti dal Sistema di Gestione della Sicurezza delle Informazioni (SGSI) del Titolare del trattamento, certificato secondo lo Standard ISO 27001, nel rispetto delle policy definite nel SGSI.*

   Le misure di sicurezza sopra elencate, in considerazione della rapidità con cui si evolvono le minacce nel settore della sicurezza informatica, sono considerate adeguate al momento, tuttavia le stesse potranno essere oggetto di futuro accordo tra le Parti per integrazioni che si dovessero rendere necessarie ***dalla normativa vigente*** *~~sulla base di valutazioni di adeguatezza da parte del Titolare e/o del Responsabile~~.*
2. *Nel valutare l'adeguatezza del livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento (o dai trattamenti), che derivano in particolare dalla distruzione, dalla perdita, dalla modifica,*

dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai Dati Personali trasmessi, conservati o comunque trattati.

3. ~~*All'esito dell'analisi dei rischi, le misure di sicurezza adeguate ai sensi dell'art. 32 del GDPR devono essere condivise ed approvate dal Titolare*~~.

Risposta

Non si conferma. La decisione è rimessa all'Amministrazione contraente in sede di stipula del contratto esecutivo.

5) Domanda

In considerazione che:

1. l'oggetto della gara riguarda oltre alle banche dati anche la fornitura del software per il calcolo delle differenze retributive e che di conseguenza lo stesso conterrà dati aziendali e del personale oggetto delle verifiche (ragione sociale azienda, nominativi dipendenti, ruoli, retribuzioni, eventuali irregolarità etc.);
2. i servizi oggetto dell'appalto sono richiesti in modalità cloud ed in quanto tali ai sensi dell'art. 17 del regolamento per le infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione (decreto direttoriale dell'Agenzia per la cybersicurezza nazionale 27 giugno 2024, n. 21007) richiedono apposita qualificazione ACN di livello 1,

si chiede conferma che tale qualifica – pur non essendo espressamente indicata - sia da intendersi implicitamente quale requisito obbligatorio di partecipazione o condizione di esecuzione del contratto.

Risposta

Vedasi *errata corrige* pubblicato in data 11/02/2026.

6) Domanda

1. La nota INL del 22 dicembre 2021 prevede che "Nel caso in cui il datore di lavoro abbia già corrisposto al lavoratore una parte della retribuzione dovuta, la stessa andrà direttamente detratta dall'importo lordo totale previsto contrattualmente (senza, quindi, alcuna operazione di "lordizzazione", trattandosi di importo da considerare già al lordo), ottenendo così il credito lordo oggetto di diffida accertativa". Premesso quanto sopra, come va intesa, al paragrafo 4.3 del Capitolato tecnico, la richiesta che il software debba essere in grado, tra l'altro, di "lordizzare le somme percepite in nero"?
2. Con riferimento al paragrafo 4.3 del Capitolato tecnico, è richiesta l'implementazione della funzionalità di "Calcolo del Part-Time INAIL". Si chiede a codesto Ente di specificare il tipo di calcolo richiesto e la sua finalità.

Risposta

1. Con riferimento alla lordizzazione dell'imponibile accertato in sede di attività ispettiva, l'applicativo deve prevedere la possibilità di effettuare elaborazioni che, in funzione della necessità dell'utente, consentano:
    a. l'applicazione della lordizzazione all'intero imponibile, ivi comprese le somme già corrisposte dal datore di lavoro anteriormente all'accertamento in assenza di busta paga e quindi dichiarate dal lavoratore;

b. l'applicazione della lordizzazione esclusivamente alla quota di imponibile oggetto di accertamento ispettivo, con separata evidenziazione dell'imponibile già erogato in precedenza ritenuto non assoggettabile a lordizzazione in quanto già inserito in busta paga.

2. La funzionalità "Calcolo del Part-Time Inail" di cui al par. 4.3 del Capitolato tecnico, deve consentire al funzionario di inserire i seguenti "dati di ingresso":

   a. ***Parametro A)***: livello, mansione e CCNL del lavoratore. Nell'ipotesi, del tutto residuale, in cui non sia disponibile un CCNL di riferimento, dovrà essere utilizzato il contratto territoriale, aziendale o individuale. In tale circostanza l'applicativo dovrà consentire l'inserimento manuale del minimo tabellare e del numero di mensilità contrattuali;

   b. ***Parametro B)*** ore di lavoro effettive svolte dal lavoratore Part-Time, comprese le ore prestate a titolo supplementare e straordinario;

   c. ***Parametro C)*** ore di assenza retribuite al lavoratore Part-Time in forza di legge o contratto come ferie, festività, permessi, infortunio, malattia, maternità e cassa integrazione.

Elaborazione effettuata dal sistema

Sulla base del **Parametro A**, l'applicativo estrae dagli archivi dei CCNL i seguenti elementi relativi al rapporto Full Time:

- il minimo tabellare mensile (limitato alla sola voce tabellare, con esclusione di contingenza, EDR, scatti di anzianità, indennità ad personam ed eventuali ulteriori voci retributive);
- il numero di mensilità contrattuali annue (13 o 14);
- il monte ore annuo del lavoratore Full Time.

Tali valori sono utilizzati per determinare la **Retribuzione media oraria**, calcolata secondo la formula:

$$\text{Retribuzione media oraria} = \frac{\text{Minimo tabellare mensile} \times \text{Mensilità annue}}{\text{Ore annue Full Time}}$$

Output del sistema

Il sistema deve restituire l'**Imponibile Convenzionale Part-Time**, sia su base mensile che annuale (a scelta indifferente), determinato come segue:

- **qualora** la Retribuzione media oraria risulti superiore al **Minimale annuale**,
  $$\text{Imponibile Convenzionale Part-Time} = \text{Retribuzione media oraria} \times (\text{Ore totali Part-Time} = B + C)$$
- **in caso contrario**,
  $$\text{Imponibile Convenzionale Part-Time} = \text{Minimale annuale} \times (\text{Ore totali Part-Time} = B + C)$$

7) Domanda

Si richiede di indicare cortesemente la data di go live per l'avvio della fornitura oggetto di gara.

Risposta

Si rimanda al par. 5.2 del Capitolato Tecnico.

8) Domanda

Con riferimento alla procedura aperta sopra riportata, richiediamo chiarimenti in merito al codice ATECO da voi inserito che risulta essere 631. Noi siamo iscritti al bando con codice ATECO 58 che ci permette di partecipare anche alle gare inerenti le banche dati. Con questi requisiti richiesti, la nostra società non può partecipare non avendo tale codice ATECO.

Risposta

Il codice ATECO riportato nel Disciplinare di gara (631 – "Elaborazione dei dati, hosting e attività connesse; portali web") non costituisce un requisito di partecipazione. Resta fermo che l'attività risultante dalla visura camerale e dall'oggetto sociale del concorrente deve essere coerente con l'oggetto dell'appalto.

9) Domanda

1. In riferimento **all'art. 4 S OBBLIGHI E ADEMPIMENTI A CARICO DEL FORNITORE**
   - **Capoverso 4** si chiede di integrare il seguente capoverso con quanto segue:
     "*Non si potrà attribuire all'Impresa responsabilità alcuna nel caso che l'inadempimento o l'errata esecuzione del Servizio sia imputabile alla mancata e/o inesatta esecuzione da parte della Committente dei propri obblighi. Nel caso che l'Impresa riceva dalla Committente informazioni errate, l'Impresa declina ogni responsabilità per il danno eventualmente occorso, anche direttamente, dalla Committente o da terzi, per i risultati prodotti sulla base di queste informazioni*".
   - **Capoverso 5** si chiede di sostituire il seguente capoverso:
     "*L'Impresa si obbliga a consentire alla Committente di procedere, in qualsiasi momento e anche senza preavviso, alle verifiche sulla piena e corretta esecuzione del presente contratto, impegnandosi ora per allora a prestare la propria collaborazione per consentire lo svolgimento di tali verifiche*".
     Con quanto segue:
     "*L'Impresa si obbliga a consentire alla Committente di procedere, alle verifiche sulla piena e corretta esecuzione del presente contratto nei limiti di 4 ore e massimo una volta all'anno; in alternativa tali verifiche potranno essere realizzate mediante idonee attestazioni e certificazioni rilasciate da enti terzi indipendenti sul sistema di gestione per la sicurezza delle informazioni (secondo norma ISO/IEC 27001-27017-27018-27035-27701) ovvero sul sistema di gestione della qualità (ISO 9001)*".

2. In riferimento **all'art. 9 S CONSEGNA DEI PRODOTTI**
   - **Capoverso 2** si chiede di sostituire il seguente capoverso:
     "Relativamente ai servizi di cui all'art. 1S, comma 1 lett. a) e b), l'Impresa, entro 5 (cinque) giorni lavorativi decorrenti dalla Data di Sottoscrizione del presente contratto, dovrà consegnare alla Committente i codici segreti delle relative licenze per l'accesso online alla ricerca, pena l'applicazione delle penali di cui all'art. 12 S".
     Con quanto segue:
     "*Relativamente ai servizi di cui all'art. 1S, comma 1 lett. a) e b), l'Impresa, entro 5 (cinque) giorni lavorativi decorrenti dalla Data di Sottoscrizione del presente contratto, dovrà consegnare alla Committente l'account e la password i per l'accesso alla piattaforma con cui vengono prestati i Servizi, pena l'applicazione delle penali di cui all'art. 12 S*".
   - **Capoverso 4** si chiede di sostituire la formulazione "**codici segreti"** con la seguente descrizione: "**credenziali di accesso".**
   - **Capoverso 5** si chiede di sostituire la formulazione "*La Committente si impegna a comunicare all'Impresa ogniqualvolta l'utente non abbia più diritto all'utilizzo del codice segreto, in modo tale che l'Impresa possa*

cancellare il suddetto codice segreto ed emetterne uno nuovo, in caso di subentro di un nuovo utilizzatore",
con la seguente descrizione:
"*La Committente si impegna a comunicare all'Impresa ogniqualvolta l'utente non abbia più diritto all'utilizzo delle credenziali di accesso, in modo tale che l'Impresa possa sostituire tali credenziali ed emetterne delle nuove, in caso di subentro di un nuovo utilizzatore.*
La Committente deve garantire la riservatezza di tutte le password per accedere alla Piattaforma, alle Applicazioni e ai Servizi, e la riservatezza delle attività effettuate utilizzando tali password. La Committente si obbliga a garantire la sicurezza del suo sistema informatico. La Committente terrà in ogni tempo manlevati e indenni l'Impresa e i suoi clienti, dipendenti e collaboratori da qualsiasi danno, spesa, costo (ivi incluse le ragionevoli spese legali), azione e/o procedimento che possa comunque derivare per effetto o in conseguenza della violazione delle garanzie che precedono. La Committente si obbliga a informare tempestivamente l'Impresa qualora venga a conoscenza di un qualsiasi uso illegale non autorizzato delle proprie password e/o account, e/o di ogni altra violazione alla sicurezza e alla riservatezza dei Dati anche solo presunta e/o di ogni altro incidente che possa compromettere il suo sistema informatico. L'Impresa potrà interrompere la prestazione dei Servizi, incluso l'accesso alla Piattaforma da parte della Committente, nel caso ricevesse segnalazioni o notizia di incidenti occorsi nei sistemi informatici della Committente che possano compromettere a giudizio dell'Impresa la Piattaforma o le altre strutture informatiche dell'Impresa o dei suoi clienti. La suddetta interruzione proseguirà fino al ricevimento della relazione sull'incidente occorso da parte della Committente, e comunque fino a che la Committente non abbia adottato tutte le misure necessarie al ripristino della sicurezza del suo sistema informatico. L'interruzione della fornitura del Servizio per i motivi ora indicati e fino al ripristino della sicurezza del sistema informatico della Committente non comporterà l'applicazione a carico dell'Impresa delle penali eventualmente previste nel Contratto".

- **Capoverso 6** si chiede di sostituire la formulazione
"*Il servizio di accesso al servizio di banca dati tramite il portale di erogazione dei servizi sarà prestato dall'Impresa tutti i giorni dell'anno per 24 ore al giorno*",
con la seguente descrizione:
"*Il servizio di accesso ai sistemi è garantito 20 ore al giorno (dalle 04.00 alle 24.00) 7 giorni su 7 - Presidio 8x5 dalle 9:00 alle 18:00 con relativo monitoraggio remoto nei periodi festivi*".

3. In riferimento **all'art. 12 S PENALI capoverso 3** si chiede di sostituire la formulazione" **codici segreti"** con la seguente descrizione: "**credenziali di accesso".**

Risposta
Non si conferma. La decisione è rimessa all'Amministrazione contraente in sede di stipula del contratto esecutivo.

Divisione Sourcing Sanità, Beni e Servizi
Il Responsabile
(*Dott. Guido Gastaldon)*

Firmato digitalmente da:
GUIDO GASTALDON
Consip S.p.A.
Firmato il 13/02/2026 17:33
Seriale Certificato: 2444
Valido dal 30/09/2024 al 30/09/2027
TI Trust Technologies QTSP CA