OGGETTO: GARA A PROCEDURA APERTA AI SENSI DEL D.LGS. 36/2023 PER L'ACQUISIZIONE DI CERTIFICATI DIGITALI– EDIZIONE 2 PER INAIL – ID 2816

I chiarimenti della gara sono visibili sui siti: www.consip.it, e www.inail.gov.it.

RISPOSTE ALLE RICHIESTE DI CHIARIMENTI

1) **DOMANDA**
In merito a quanto indicato a pag. 18 del Capitolato Tecnico relativamente alla gestione dei segreti dei dispositivi fisici e dei certificati di firma remota, la Certification Authority prevede l'inoltro di tali quantità attraverso canali digitali quali SMS e e-mail. Si chiede di confermare la rispondenza di tale modalità di gestione con le esigenze dell'Istituto.
Risposta
Posto che il quesito non è chiaro si evidenzia quanto previsto al paragrafo 4.2.1 secondo cui il Fornitore dovrà effettuare la consegna delle *"… credenziali di autenticazione al servizio di firma remota"* che dovranno essere *"**opportunamente protette**"*. Pertanto indipendentemente dalla modalità di invio l'importante è che tali credenziali siano opportunamente protette.

2) **DOMANDA**
In merito alla gestione degli strumenti per la 2FA, a pagina 15 del Capitolato Tecnico si legge che per la gestione dei codici OTP l'Istituto prevede soltanto l'utilizzo della modalità tramite APP. Successivamente però si fa riferimento a token OTP, definiti nel Capitolato Tecnico come dispositivi hardware personali in grado di visualizzare codici OTP da utilizzare per l'autenticazione al sistema di firma remota. Si chiede di confermare che l'unica modalità di gestione dei codici OTP prevista sia quella tramite APP e quindi di considerare come refuso i riferimenti ai dispositivi hardware.
Risposta
Si conferma

3) **DOMANDA**
Viste le indicazioni del CAB-Forum, a cui la Certification Authority si attiene per la emissione e gestione dei certificati SSL, la durata massima consentita per i certificati SSL server è 12 mesi. Si chiede di confermare che quanto riportato nel Capitolato Tecnico in merito alla durata di 36 mesi dei certificati SSL server sia una indicazione che i certificati stessi debbano essere attivi per tutta la durata del contratto, previo rinnovo annuale
Risposta
Si conferma, fermo restando che il rinnovo del certificato è automatico.

4) **DOMANDA**
Non essendovi nel Disciplinare di Gara riportate le numeriche e il valore economico da base d'asta per i certificati SSL server e Code Signing, si chiede di confermare che l'Istituto intenda richiedere alla Committente di emettere certificati SSL server e Code Signing da portale web dedicato e che tale fornitura verrà contrattualizzata separatamente. In caso contrario si chiede di indicare il numero di certificati e il valore di base d'asta per ogni tipologia indicata nel paragrafo 4.1.2 del Capitolato Tecnico;
Risposta
Non si conferma. La fornitura di cui al quesito è inclusa nel servizio online, come si evince dal paragrafo 4.1 e relativi sottoparagrafi del Capitolato Tecnico. Per i dati relativi all'erogato pregresso si può fare riferimento alle indicazioni fornite al paragrafo 2, e relativi sottoparagrafi, del medesimo Capitolato Tecnico.

5) DOMANDA

Si chiede di confermare che al Fornitore venga richiesto di rendere disponibili per i servizi oggetto della presente iniziativa le API REST o i web services SOAP al fine di consentirne la integrazione applicativa con la piattaforma dell'Istituto. Si chiede altresì di confermare che eventuali attività di sviluppo debbano considerarsi in carico al reparto DCOD dell'Istituto stesso, con supporto tecnico specialistico da parte del Fornitore;

Risposta

Si conferma la prima domanda. Con riferimento alla seconda domanda si precisa che come previsto dal paragrafo 3 del Capitolato Tecnico, il *"Fornitore aggiudicatario della presente iniziativa dovrà supportare l'Istituto nell'aggiornamento del layer di integrazione senza alcun onere aggiuntivo"*..

6) DOMANDA

Viste le mutate condizioni del quadro tecnico e normativo rispetto a quando sono stati introdotti sul mercato i dispositivi wireless ed essendo oggi possibile accedere ai portali della Pubblica Amministrazione anche con altri strumenti come SPID, CIE, nodo FICEP eIDAS, si chiede, contrariamente a quanto indicato nel paragrafo 4.3 del Capitolato Tecnico, se possa essere rispondente con le esigenze dell'Istituto la fornitura di dispositivi crittografici USB standard, non wireless, che garantiscano, comunque, la possibilità di sottoscrivere documenti in modalità offline. In tal caso si chiede di confermare la possibilità di riportare il prezzo dei dispositivi crittografici USB standard per la voce "Dispositivi fisici di firma digitale con CNS (comprensivi di manutenzione)" prevista nella tabella 2 Par. 3 del Disciplinare di Gara;

Risposta

Non si conferma.

7) DOMANDA

Vista l'indicazione di "(opzionale)" accanto alla descrizione della fornitura di SPID Professionali e SPID intestato a persona Giuridica riportati nella tabella 1 Par. 3 del Disciplinare di Gara, si chiede conferma che tali servizi possano essere offerti solo opzionalmente dal concorrente. Si chiede di confermare se le identità SPID oggetto della presente iniziativa possano essere considerate opzionali e quindi anche non inseribili in offerta come sembra essere indicato nel Disciplinare di Gara. In caso di risposta affermativa chiediamo conferma che all'interno dell'offerta economica si possa indicare il valore unitario pari a zero. In caso di risposta negativa si chiede di specificare se tali servizi debbano essere considerati di tipo 2 e 3;

Risposta

Non si conferma. Opzionale significa che la Committente si riserva di acquisire tali servizi. Quanto al tipo si richiama quanto previsto al par. 4.1.2.3 del Capitolato Tecnico, ossia "*Il Fornitore dovrà garantire l'eventuale richiesta da parte di INAIL della fornitura di* ***SPID professionali*** *e* ***SPID intestato a persona giuridica****, nelle quantità previste dal Disciplinare di Gara. Entrambe le fattispecie di identità digitale dovranno essere sempre* ***conformi alla normativa vigente in materia***".

8) DOMANDA

Al fine di consentire la massima aderenza e un maggior controllo sulla gestione dei requisiti normativi e di sicurezza dei servizi oggetto della presente iniziativa, si chiede se possa essere considerato rispondente con le esigenze dell'Istituto l'utilizzo di pannelli diversificati per i servizi di emissione e firma, eventualmente integrabili, mediante apposite API, con la piattaforma dell'Istituto;

Risposta

Il quesito non è molto chiaro, in particolare non si comprende il significato della parola "pannelli". Tuttavia si rimanda ai paragrafi 4.1.1 e 4.1.2 e si precisa che i rispettivi portali possono essere diversi purché integrabili con la piattaforma dell'Istituto.

9) **DOMANDA**

Viste le disposizioni eIDAS2 che limitano a 5 anni la durata delle certificazioni di conformità QSCD delle smartcard e visto che i certificati di firma a 3 anni, oggetto della presente iniziativa, potranno essere emessi fino all'ultimo giorno di validità del contratto, si comunica che le smartcard, contenute nei dispositivi USB, nel corso della fornitura saranno soggette a ricertificazione. In caso di revoca della certificazione di conformità QSCD, la Certification Authority dovrà revocare i certificati emessi sui dispositivi e l'Istituto dovrà provvedere all'approvvigionamento di nuovi dispositivi e certificati con relativi costi a proprio carico. Si chiede di confermare che quanto indicato sia in linea con quanto previsto dall'Istituto. Diversamente si richiede di specificare come l'Istituto intenda gestire i dispositivi con smart card con certificazione di conformità QSCD eventualmente revocata.

Risposta

Non si conferma. Si rimanda al par. 3 del Capitolato tecnico ove è previsto che per "*l'intera durata contrattuale dovrà essere assicurata la validità di tutti i certificati senza oneri aggiuntivi, nonché l'aggiornamento tecnologico dei dispositivi di firma e l'adeguamento alla normativa in corso di vigenza*".

10) **DOMANDA**

In merito alla fornitura dei dispositivi fisici CNS si chiede di confermare che i dispositivi dovranno essere consegnati in un singolo lotto. In caso contrario si chiede di specificare la minima quantità ordinabile per singola richiesta;

Risposta

Si conferma

11) **DOMANDA**

Si chiede di confermare che nel prezzo di base d'asta per le firme temporanee per utilizzo one shot (use e getta) non sia da ritenersi incluso il costo da riconoscere agli IDP per eventuali identificazioni tramite SPID;

Risposta

La base d'asta delle firme temporanee per utilizzo one-shot è relativa al solo certificato usa e getta.

12) **DOMANDA**

Si chiede di confermare che i certificati CNS e di firma remota, digitale e automatica oggetto della fornitura possano essere emessi utilizzando profili con validità a 36 mesi.

Risposta

Posto che non è chiaro cosa si intenda per "profili con validità a 36 mesi", i certificati dovranno essere validi per l'intera durata contrattuale.

13) **DOMANDA**

Schema di Contratto – Condizioni Generali:

Con riferimento all'art. 3G, paragrafo 7, si chiede alla committente di precisare in che termini e modalità potrebbero avvenire le verifiche circa il rispetto dell'applicazione di quanto previsto in capo al responsabile del contratto.

Risposta

Le verifiche, che potranno essere attivate dalla Committente in via solamente eventuale, avranno ad oggetto la corretta applicazione, da parte del Responsabile del Contratto (o Responsabile Unico delle Attività Contrattuali), di quanto previsto dal comma 6 del medesimo art. 3G delle Condizioni Generali e quindi la corretta applicazione di "*tutte le necessarie procedure organizzative*" e degli "*opportuni flussi comunicativi*" ivi previsti.

14) DOMANDA

Schema di Contratto – Condizioni Generali:

Con riferimento all'art. 4G si prega di confermare che l'obbligo di riservatezza potrà essere eccezionalmente derogato laddove la divulgazione da parte dell'impresa di informazioni e/o dati attinenti al contratto debba avvenire sulla base di un ordine, provvedimento o procedimento dinanzi ad una pubblica autorità, di cui l'impresa abbia dato tempestiva comunicazione alla committente.

Risposta

Si conferma limitatamente ai casi in cui l'ostensione di informazioni e/o dati attinenti al contratto è prescritta in un ordine o provvedimento di una Pubblica Autorità.

15) DOMANDA

Schema di Contratto – Condizioni Generali:

Con riferimento all'articolo 10 G, paragrafo 4, si chiede di confermare che prima che la committente possa incamerare la garanzia i danni saranno accertati con sentenza definitiva o provvedimento equivalente dalle autorità competenti.

Risposta

Non si conferma.

16) DOMANDA

Schema di Contratto – Condizioni Generali:

Con riferimento all'art. 11 G, paragrafo 5, che recita "Con riferimento alla previsione di cui all'art. 23.5 dello schema di contratto che recita: "*Dalla data di efficacia del recesso, l'Impresa dovrà cessare tutte le prestazioni contrattuali, assicurando che tale cessazione non comporti danno alcuno alla Committente e/o all'Amministrazione*", si chiede gentilmente alla Spett. Stazione Appaltante di voler:

i. confermare che, nel caso in cui la Committente eserciti il diritto di recesso, in considerazione della cessazione del rapporto contrattuale, incluso l'aspetto del trattamento dei dati, l'Impresa non sarà tenuta a continuare a erogare le prestazioni oggetto del contratto;
ii. in subordine, confermare che, nel caso in cui l'Impresa sia tenuta a continuare a erogare le prestazioni oggetto del contratto su espressa richiesta della Committente, l'Impresa stessa avrà diritto a ricevere i relativi corrispettivi previsti dal contratto.

Risposta

Si conferma che, come previsto nella richiamata previsione delle Condizioni Generali, "*dalla data di efficacia del recesso, l'Impresa dovrà cessare tutte le prestazioni contrattuali, assicurando che tale cessazione non comporti danno alcuno alla Committente e/o all'Amministrazione. La Committente effettuerà la verifica di conformità delle prestazioni sino a quel momento eseguite*". In relazione al trattamento dei dati personali, alla cessazione del contratto, cesserà, parimenti, anche il predetto trattamento. L'aggiudicatario dovrà, restituire le informazioni personali in suo possesso e, conseguentemente, cancellarle dai propri data base, salvo gli eventuali obblighi di legge che ne impongano la conservazione. Restano ferme le previsioni relative al grace period.

17) DOMANDA

Schema di Contratto – Condizioni Generali:

Con rifacimento all'art 17 G, paragrafo 4, e nello specifico all'inciso […] *Acquisite e valutate negativamente le controdeduzioni […]*" si chiede di precisare quali saranno i parametri in base ai quali la committente procederà ad effettuare tale valutazione.

Risposta

Non possono essere individuati dei parametri certi sulla cui base procedere alla valutazione delle controdeduzioni in caso di risoluzione. E' evidente, infatti, che la Committente si riserva di effettuare le proprie valutazioni in ragione del caso specifico e sulla base delle circostanze reali che hanno dato luogo alla risoluzione.

18) DOMANDA

Schema di Contratto – Condizioni speciali

Con riferimento all'art 2S, paragrafo 1, letto in combinato disposto con l'art. 3 ("OGGETTO E DURATA DEL CONTRATTO") del Capitolato tecnico, si chiede di confermare che la durata dei servizi oggetto di fornitura, in particolare i servizi di firma, sia quella indicata nel presente articolo e decorrente dalla sottoscrizione del contratto e non dall'attivazione delle singole firme.

Risposta

All'art. 2S delle Condizioni Speciali è previsto che "*Il presente contratto spiega i suoi effetti dalla data della sua sottoscrizione ed avrà termine allo spirare di 36 mesi decorrenti dalla "Data di accettazione della Fornitura"* ***da intendersi quale data di messa in esercizio del servizio online****, come disciplinato dal Capitolato Tecnico*". Tenuto conto altresì di quanto previsto ai paragrafi 4.2.1 e 5 del Capitolato Tecnico, la decorrenza della durata contrattuale deve intendersi dalla data di messa in esercizio del servizio online.

19) DOMANDA

Schema di Contratto – Condizioni speciali

Con riferimento all'art. 9S, paragrafo 5, si chiede di precisare in che cosa consistono tali verifiche e altresì di confermare che le stesse siano volte limitatamente a verificare il rispetto dei requisiti di cui alla documentazione di gara.

Risposta

Come previsto al medesimo art. 9S, paragrafo 5, delle Condizioni Speciali, le verifiche ivi previste dovranno essere svolte "*su tutte le prestazioni contrattuali*" e "*mediante verifica e approvazione di ciascun report di cui al paragrafo 4.2.3 del Capitolato Tecnico*".

20) DOMANDA

Schema di Contratto – Condizioni speciali

Con riferimento all'art 9 S, paragrafo 10, si chiede di confermare la disapplicazione della previsione rispetto all'affidamento in parola.

Risposta

Non si conferma.

21) DOMANDA

Schema di Contratto – Condizioni speciali

Con riferimento all'art 10 S - Tabella, si chiede di indicare i riferimenti al capitolato essendo presente la seguente dicitura "Errore- riferimento non trovato".

Risposta

La tabella completa è riportata in modo identico nel par. 6 del Capitolato Tecnico con i riferimenti visibili.

22) DOMANDA

Schema di Contratto – Condizioni speciali

Con riferimento all' Art. 10 S, paragrafo 5, si chiede di precisare cosa si intende per gli eventuali periodi di sperimentazione delle Applicazioni.

Risposta

Si intendono periodi iniziali di messa in esercizio di nuove applicazioni per la firma.

23) DOMANDA

Premesso che nella scheda economica che occorre compilare all'interno della procedura telematica sul sito acquistinretepa.it non vi sono gli spazi per l'inserimento dei costi della manodopera e degli oneri per la sicurezza aziendali, chiediamo conferma che l'operatore economico NON debba indicarli. In caso contrario chiediamo di predisporre apposito/i campo/i oppure di indicare una modalità alternativa attraverso cui inviarli;

Risposta

Si conferma. Come emerge anche dal paragrafo 3 del Capitolato d'Oneri, la gara ha ad oggetto esclusivamente servizi di natura intellettuale e forniture senza posa in opera.

24) DOMANDA

Chiediamo cortesemente di allegare il patto di integrità di Inail o di indicare il link dove è possibile prenderne visione. Da una nostra ricerca su Web non siamo riusciti ad individuarlo.

Risposta

Il link è il seguente:

https://www.inail.it/portale/it/atti-e-documenti/note-provvedimenti-e-istruzioni-operative/normativa-delibere-cs/dettaglio.2024.02.delibera-comm-straord-n-35-del-20-feb-2024.html

25) DOMANDA

CONDIZIONI DI CONTRATTO GENERALI

Si chiede conferma che gli unici servizi oggetto della procedura di gara che possono contemplare il trattamento dati da parte del fornitore in qualità di Responsabile siano solo i servizi di firma digitale e che qualora detti servizi contemplino il trattamento dati personali da parte del fornitore in qualità di Responsabile, tale aspetto verrà comunicato da una delle Parti in sede di aggiudicazione.

Risposta

Non si conferma. I servizi oggetto del contratto comportano il trattamento di dati personali, pertanto il Fornitore sarà nominato Responsabile del trattamento e dovrà rispettare le obbligazioni contenute nell'art. 16S del Contratto – Condizioni Speciali.

26) DOMANDA

CONDIZIONI DI CONTRATTO GENERALI

Si chiede conferma che, vista la sussistenza di 2 nomine a Responsabile del trattamento (Contratto Speciali art. 16S e Allegato Privacy), al rapporto tra le Parti si applicherà unicamente la nomina a responsabile prevista da Contratto Speciali art. 16 S.

Risposta

Si conferma. Il Fornitore aggiudicatario, pertanto, verrà designato in qualità di Responsabile esterno attraverso la nomina prevista dall'art. 16S del Contratto – Condizioni Speciali.

27) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art 16 S n. 6 lett. e) ed f) che dispone che:

"Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default).

f) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;"

si prega di confermare che le misure richieste al Responsabile saranno conformi a quanto contrattualmente pattuito tra le Parti.

Risposta

A tal riguardo si evidenzia che, dal punto di vista del trattamento dei dati personali, il Fornitore dovrà essere in possesso delle garanzie adeguate, che riguardano anche il rispetto dei principi di privacy by design e privacy by default. Inoltre, il Fornitore deve adottare misure di sicurezza adeguate come prescritto dalla normativa vigente. Come evidenziato nel comma 7 dell'art. 16S "*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 (…) e deve presentare il Piano di sicurezza e l'implementazione delle relative contromisure, conformemente al principio di privacy by design ex art. 25 del GDPR*".

28) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 6 lett. i) che dispone che:

"Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE."

Si prega di confermare che gli obblighi posto a carico del Responsabile dalla previsione potranno essere letto conformemente a quanto stabilito al riguardo dall'art. 28, comma 3 lett. f) GDPR.

Risposta

Non si conferma.l Fornitore aggiudicatario dovrà collaborare con l'Amministrazione, per quanto di propria competenza in relazione ai servizi svolti, per l'adempimento degli obblighi di cui agli artt. da 31 a 36 del Regolamento UE 2016/679.

29) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 7 che dispone che:

"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 e l'implementazione delle relative contromisure, conformemente al principio di privacy by design ex art. 25 del 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."

Si chiede conferma che le misure che dovranno essere implementate dal Responsabile saranno quelle indicate nel contratto.

Risposta

Si veda la risposta al quesito n. 27) e le previsioni di cui all'art. 16S n. 7

30) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 9 che dispone che:

"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. Nel caso in cui tali garanzie risultassero insussistenti o inidonee la Committente potrà risolvere il contratto con il Responsabile iniziale."

Si prega di confermare che il riferimento al Sub-Responsabile sia unicamente al Responsabile iniziale in quanto unica controparte della Committente nel contratto avente ad oggetto i servizi resi.
Nella denegata ipotesi in cui il riferimento al Sub-Responsabile sia corretto, si chiede di confermare che le audit/ispezioni saranno effettuati:
1) nei limiti di cui all'art. 28 comma 3 lett. h) del GDPR;
2) previo accordo sui tempi e sulle modalità di dette verifiche e purché le stesse non comportino l'analisi dei dati di terze parti e non collidano con obblighi di riservatezza assunti dal Responsabile o dal sub-responsabile e con le policy di questi ultimi;
3) nella misura massima di una volta l'anno, con preavviso di almeno 20 (venti) giorni e a valle di apposito accordo di riservatezza (NDA) fornito dal sub-Responsabile;
4) nel caso in cui il Titolare si avvalga di auditor esterno quest'ultimo deve essere un auditor qualificato e concordato tra le Parti;
5) i costi di tali audit saranno a carico del Titolare;
Si prega altresì di confermare che nel caso in cui, a fronte di tali audit e ispezioni, dovessero emergere non conformità, la Committente, prima di risolvere il contratto con il Responsabile iniziale, assegnerà al Sub-Responsabile e/o al Responsabile un termine congruo entro il quale questi ultimi potranno rimuovere le non conformità riscontrate e che, in ogni caso, la Committente risolverà il contratto solo in presenza di non conformità tali da impedire l'esecuzione dei servizi contrattuali.

Risposta

Con riferimento ai soggetti nei riguardi dei quali la Committente si riserva di svolgere audit e ispezioni, si evidenzia che il comma 9 dell'art. 16S si riferisce sia al Responsabile iniziale che al sub-responsabile.
In merito alle modalità con le quali l'Amministrazione può procedere alle predette attività di controllo, si sottolinea che queste ultime avverranno in conformità a quanto previsto dal comma 15 dell'art. 16S.
Per quanto concerne la risoluzione si applica il comma 10 dell'art. 16S.

31) DOMANDA

CONTRATTO CONDIZIONI SPECIALI
Con riferimento all'art. 16 S n. 10 che dispone che:
"10. Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, la Committente applicherà al Fornitore/Responsabile Inziale del trattamento la penale di cui all'art. __ S e diffiderà lo stesso a far adottar al sub-Responsabile del trattamento tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, la Committente potrà risolvere il contratto con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno."
si chiede conferma che, vista la carenza di riferimenti allo specifico articolo applicabile, si chiede conferma della inapplicabilità della presente previsione in relazione alla nomina a Responsabile e che, in materia di penali, si farà riferimento a quanto esplicitamente indicato nel contratto tra le Parti anche rispetto a modalità e tempi di applicazione delle penali.

Risposta

Non si conferma l'inapplicabilità della previsione richiamata nel quesito. Le penali sono espressamente indicate all'art. 10S delle Condizioni Speciali ("Penali"), ai commi 2 e 3.

32) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 11 che dispone che:

"11. 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."

Si chiede conferma che in materia di responsabilità e risarcimento le Parti rimanderanno a quanto indicato nell'art. 82 del GDPR e che, conformemente a quanto disposto dallo stesso art. 82 GDPR, il Titolare potrà azionare la manleva nel caso in cui la responsabilità del Responsabile sia stata positivamente riconosciuta sulla base di un provvedimento giudiziale o altro provvedimento equiparabile.

Risposta

Si conferma. La manleva, in conformità all'art. 82 del Regolamento UE 2016/679, potrà essere azionata in base ad un provvedimento giurisdizionale o altro provvedimento equiparabile, quale, ad esempio, quello del Garante per la protezione dei dati personali.

33) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 12 che dispone che:

"12. Il Responsabile del trattamento deve assistere il Titolare del trattamento al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. da 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze al Titolare del Trattamento, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti."

si chiede conferma che tale richiesta sia da intendersi per quanto di competenza del Responsabile secondo il contratto in essere tra le Parti e nei limiti di quanto indicato nell'art. 28, comma 3, lett. e) del GDPR.

Risposta

Si conferma.

34) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 12 che dispone che:

"Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali,

entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile del trattamento e/o di suoi sub-Responsabili.
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."
Si chiede conferma che quanto sopra richiesto sia limitato a quanto indicato nell'art. 28, comma 3, lett. f) e nell'art 33 comma 2 GDPR.

Risposta

Si evidenzia che la collaborazione richiesta al Fornitore in caso di data breach è quella prevista dalla legge (art. 28 comma 3, lett. f) e art. 33 del Regolamento). L'Amministrazione potrà riservarsi di richiedere ogni ulteriore informazione - connessa alle attività svolte dall'aggiudicatario – che dovesse ritenere utile ai fini della valutazione dell'episodio e della comunicazione dell'evento al Garante ed eventualmente agli interessati del trattamento.

35) DOMANDA

CONTRATTO CONDIZIONI SPECIALI
Con riferimento all'art. 16 S n. 15 che dispone che:
"15. 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. A tal fine, il Titolare informa preventivamente il Responsabile del trattamento con un preavviso minimo di tre 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. ___ 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.
22. 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."

premesso che l'art. 16 S prevede il diritto di audit/ispezione da parte del Titolare anche al paragrafo n. 9 dello stesso, si chiede di confermare che le audit/ispezioni di cui ai paragrafi n. 15 e 22 dell'articolo saranno effettuati nel rispetto delle seguenti modalità:

1) nei limiti di cui all'art. 28 comma 3 lett. h) del GDPR;

2) previo accordo sui tempi e sulle modalità di dette verifiche e purché le stesse non comportino l'analisi dei dati di terze parti e non collidano con obblighi di riservatezza assunti dal Responsabile o dal sub-responsabile e con le policy di questi ultimi;

3) nella misura massima di una volta l'anno, con preavviso di almeno 20 (venti) giorni e a valle di apposito accordo di riservatezza (NDA) fornito dal sub-Responsabile;

4) nel caso in cui il Titolare si avvalga di auditor esterno quest'ultimo deve essere un auditor qualificato e concordato tra le Parti;

5) i costi di tali audit saranno a carico del Titolare.

Si prega altresì di confermare che:

- nel caso in cui, a fronte di tali audit e ispezioni, dovessero emergere non conformità, la Committente, prima di risolvere il contratto con il Responsabile iniziale, assegnerà al Sub-Responsabile e/o al Responsabile un termine congruo entro il quale questi ultimi potranno rimuovere le non conformità riscontrate e che, in ogni caso, la Committente risolverà il contratto solo in presenza di non conformità tali da impedire l'esecuzione dei servizi contrattuali;
- vista la carenza di riferimenti allo specifico articolo applicabile, la penale citata dalla previsione non sarà applicabile in relazione alla nomina a Responsabile e che, in materia di penali, si farà riferimento a quanto esplicitamente indicato nel contratto tra le Parti al riguardo anche rispetto a modalità e tempi di applicazione.

Risposta

Quanto alle penali si veda la risposta al precedente quesito n. 31). In merito alle attività di audit e ispezioni si richiama il riscontro al quesito n. 30).

36) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 17 che dispone che:

"17. Al termine della prestazione dei servizi oggetto del contratto, il Responsabile su richiesta del Titolare, si impegna a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione."

Si chiede di confermare che eventuali supporti rimovibili (qualora previsti nei servizi di cui al contratto tra le Parti) saranno restituiti ove di proprietà del Titolare secondo modalità e tempi concordati tra le Parti.

Risposta

Si conferma.

37) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 20 che dispone che:

20. Su richiesta del Titolare, il Responsabile 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.

considerata la natura volontaria dell'adesione a codici di Condotta e dell'ottenimento di Certificazioni di cui agli art. 40 e 42 del GDPR, che implicherebbero un effort al di fuori del perimetro contrattuale tra le Parti, si prega di confermare che l'adesione da parte del Responsabile a detti codici di condotta o l'ottenimento di dette certificazioni non costituiscano un requisito obbligatorio a carico del Responsabile e che, in caso di richiesta del Titolare, le Parti ne negozieranno preventivamente le relative modalità di implementazione.

Risposta

Tenuto conto del tenore della previsione richiamata, qualora il Titolare ne faccia richiesta, il Responsabile sarà tenuto a fornire le ulteriori garanzie ivi previste, fermo restando che si conferma che le Parti potranno negoziarne preventivamente le relative modalità di implementazione.

38) DOMANDA

CONTRATTO CONDIZIONI SPECIALI

Con riferimento all'art. 16 S n. 24 che dispone che:

"24 Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti."

Si chiede di confermare che eventuali nuove misure, diverse da quelle contrattualmente pattuite, dovranno essere preventivamente concordate tra le Parti.

Risposta

Si conferma.

39) DOMANDA

ALLEGATO PRIVACY

Nella denegata ipotesi in cui venisse confermata l'applicazione del documento "Allegato Privacy", con riferimento alle seguenti previsioni dello stesso che dispongono che:

"SICUREZZA DEI DATI PERSONALI, p.2

Il Fornitore ottempererà a tutte le norme in materia di Trattamento dei Dati Personali in relazione al Trattamento dei Dati Personali ivi comprese quelle che saranno emanate nel corso della durata del Contratto al fine di assicurare, ciascuno nell'ambito delle proprie attività e competenze specifiche, un adeguato livello di sicurezza dei trattamenti, inclusa la riservatezza e in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale,

modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta.
"OBBLIGHI E ISTRUZIONI PER IL FORNITORE
I. OBBLIGHI GENERALI DEL FORNITORE
(..) 2. A tal fine il Fornitore si impegna a:
- (..)- adottare, Misure di sicurezza come di seguito previste e in ogni caso adeguate a garantire la protezione e la sicurezza dei Dati Personali al fine di prevenire a titolo indicativo e non esaustivo:
- incidenti di sicurezza; violazioni dei Dati Personali (Data Breach)
- ogni violazione delle misure di sicurezza;
- tutte le altre forme di Trattamento dei dati non autorizzate o illecite."
Si chiede conferma che le misure che dovranno essere implementate dal Responsabile saranno quelle indicate nel contratto e/o che eventuali nuove misure, diverse da quelle contrattualmente pattuite, dovranno essere preventivamente concordate tra le Parti.

Risposta

Si veda la risposta al precedente quesito n. 26). Si faccia riferimento altresì alle risposte ai precedenti quesiti nn. 27), 29) e 38).

40) DOMANDA

ALLEGATO PRIVACY
Nella denegata ipotesi in cui venisse confermata l'applicazione del documento "Allegato Privacy", con riferimento alla seguente previsione dello stesso che dispone che:
"IV. COLLABORAZIONE DEL FORNITORE NELL'ADEMPIMENTO DEGLI OBBLIGHI DEL TITOLARE
Il Fornitore assiste il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento."
Si prega di confermare che gli obblighi posto a carico del Responsabile dalla previsione potranno essere letti conformemente a quanto stabilito al riguardo dall'art. 28, comma 3 lett. f) GDPR.

Risposta

Si veda la risposta al precedente quesito n. 26). Si veda altresì la risposta al precedente quesito n. 28).

41) DOMANDA

ALLEGATO PRIVACY
Nella denegata ipotesi in cui venisse confermata l'applicazione del documento "Allegato Privacy", con riferimento alle seguenti previsioni dello stesso che dispongono che:
"IV.A) Misure di sicurezza.
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:
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 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 sulla base di valutazioni di adeguatezza da parte del Titolare e/o del Responsabile."
"VII. MODIFICHE DELLE LEGGI IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI
In caso di modifica delle Norme in materia di Trattamento dei Dati Personali applicabili al trattamento dei Dati Personali, il Fornitore e il Titolare collaboreranno, per quanto di propria competenza, affinché siano sviluppate, adottate e implementate misure di adeguamento al GDPR e alle sue successive modifiche e integrazioni durante il periodo di efficacia del Contratto."
si prega di confermare che le misure richieste al Responsabile saranno conformi a quanto contrattualmente pattuito tra le Parti e che, nel caso di integrazioni oggetto di eventuale accordo aggiuntivo, i contenuti di quest'ultimo saranno negoziati tra le Parti.

Risposta

Si veda la risposta al precedente quesito n. 39).

42) DOMANDA

ALLEGATO PRIVACY
Nella denegata ipotesi in cui venisse confermata l'applicazione del documento "Allegato Privacy", con riferimento alle seguenti previsioni dello stesso che dispongono che:
"V. ULTERIORI OBBLIGHI DI GARANZIA DEL FORNITORE (..)
Il 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, 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.
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.
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."
Si chiede conferma che in materia di responsabilità e risarcimento le Parti rimanderanno a quanto indicato nell'art. 82 del GDPR e che, conformemente a quanto disposto dallo stesso art. 82 GDPR, la Parte adempiente potrà azionare la manleva nel caso in cui la responsabilità della Parte inadempiente sia stata positivamente riconosciuta sulla base di un provvedimento giudiziale o altro provvedimento equiparabile.

Risposta

Si veda la risposta al precedente quesito n. 26). Si veda altresì la risposta al precedente quesito n. 32)

Divisione Sourcing Digitalizzazione

Il Responsabile

(Ing. Patrizia Bramini)