Allegato (B)

CARATTERISTICHE DEI SERVIZI RICHIESTI

Acquisizione di Servizi specialistici di supporto anche informatico alle attività di vigilanza e controllo dei Servizi Antisofisticazioni Agroalimentare di cui al Titolo V "Contrasto alle frodi" della l.r. n. 1 del 22 gennaio 2019

Sommario

TITOLO I
CARATTERISTICHE DEL SERVIZIO RICHIESTO

I ***Servizi specialistici di supporto alle attività di vigilanza e controllo dei Servizi Antisofisticazioni Agroalimentare*** richiesti sono legati all'implementazione del disposto di legge di cui all'art. 52 comma 2 lettera d), e), f) della l.r. n. 1/2019 e più in generale alle attività di monitoraggio, vigilanza e presidio del territorio previste dal titolo V "Contrasto alle frodi" della medesima legge.
Le prestazioni riguardano, tra le altre cose, il mantenimento, aggiornamento e sviluppo della piattaforma internet denominata "Portale SAA", istituita con l'art. 53 comma 1 lettera e) della citata l.r. 1/2019. Il portale è inteso quale supporto alle attività di vigilanza e controllo svolte dai Servizi Antisofisticazioni Agroalimentare.

1. Risultati attesi dal servizio richiesto - Intendimenti e obiettivi di carattere essenziale.

Con l'acquisizione del servizio la PA intende conseguire l'obiettivo di proseguire il processo di modernizzazione degli strumenti operativi messi a disposizione dei SAA avviato nel 2017 dalla Direzione Agricoltura e, al contempo, dotarsi dei mezzi e delle professionalità utili a sostenere l'attuazione di quanto disposto al Titolo V "Contrasto alle frodi" della l.r. del 22 gennaio 2019 n. 1.
I risultati che la stazione appaltante si attende dall'acquisizione dei servizi oggetto del presente documento consistono nel:

a) mantenere in efficienza, migliorare e aggiornare e ulteriormente sviluppare tutte le funzioni della piattaforma "Portale SAA": "*Sistema di monitoraggio dell'E-commerce*"; "*Sistema per la gestione dei reperti APR (Aeromobile a Pilotaggio Remoto*"; "*Sistema di archiviazione e catalogazione dei referti delle analisi chimico-fisiche e isotopiche e dei verbali di contestazione e constatazione*"; "*Sistema di compilazione guidata dei verbali di Constatazione e Contestazione*"; "*Sistema di gestione delle attività dei SAA (Agenda) idoneo al coordinamento e alla pianificazione delle azioni di vigilanza e controllo*"; "*Database dei vini venduti tramite internet correlato alle informazioni conservate nel portale*" *(denominato sistema MEC - Monitoraggio E-Commerce); APP ibrida multifunzione dedicata all'acquisizione di immagini di supporto alla compilazione dei verbali nonché connessa al database dei SAA; sistemi di verifica formale dei dati riportati nelle etichette di prodotti vinari.* Detti strumenti devono essere mantenuti efficienti, funzionali, aggiornati e implementati sia a livello di codice informatico (anche per quanto riguarda l'aggiornamento ai migliori standard di sicurezza), che di contenuti;
b) mantenere operativo, migliorare e aggiornare il sistema MEC (secondo il processo *standard* individuato alla lettera g) del punto 2, sia a livello di codice informatico che di contenuti;
c) implementare il portale delle funzioni necessarie a dare seguito al dettato del comma 2 art. 52 della l.r. 1/2019. Le nuove funzioni, dovranno essere sviluppate in aderenza ai requisiti prestazionali del Portale SAA di cui al punto 4 del presente documento, e dovranno permettere l'assorbimento e la conservazione dei dati recuperati dai soggetti di cui alla lettera f) del citato articolo di legge nonché l'elaborazione dei dati e la produzione del "documento riassuntivo";
d) acquisire ulteriori servizi specialistici di supporto alle attività dell'Ufficio di Coordinamento SAA e dei SAA.

2. Obiettivi specifici che si intendono conseguire con il servizio richiesto e modalità di realizzazione per ambito d'attività; illustrazione, non esaustiva, ma di carattere essenziale.

Gli obiettivi di risultato espressi al punto precedente sono perseguiti anche tramite lo svolgimento di attività più specifiche tra le quali figurano il potenziamento e l'implementazione sia dal punto di vista informatico sia informativo funzionale di tutte le funzionalità del portale, tra le più importanti figurano le attività relative al:

a) ***Portale SAA***
Il portale deve essere mantenuto in attività ed efficienza e tutte le sue funzioni mantenute aggiornate e operative nonché migliorate nelle sue funzionalità secondo le linee già adottate nel suo sviluppo. Il sistema deve mantenere un'interfaccia di facile utilizzo, ad accesso differenziato a seconda della profilazione dell'utente con layout a menù laterale (espandibile/collassabile), videate scalate per funzione e utente con pulsanti di ingresso alle successive a seconda dell'utente loggato.

b) ***Funzione di archiviazione, catalogazione, composizione documenti condivisa (Portale SAA).***
Sono mantenute in efficienza, migliorate e aggiornate le funzioni relative: all'archiviazione ottica dei verbali redatti dai SAA e dei referti delle analisi chimico-fisiche e isotopiche dei campioni prelevati e sottoposti ad analisi, nonché dell'ulteriore documentazione presente (video, audio, foto, etc.); alle funzioni di ricerca, di catalogazione avanzata dei documenti per parole chiave e la correlazione in base alla denominazione giuridica al prodotto monitorato; alla restituzione dei dati presenti in forma di rapporto testuale, grafica e statistica; alla composizione di documenti condivisi (composizione multiutente); alle funzionalità legate all'upload multi selezione (più files contemporaneamente) e multi file (gestione formati video, foto, audio, pdf, testo); alla parziale informatizzazione dei processi legati all'operatività dei SAA, ivi compresa la stampa dei verbali di constatazione, contestazione e prelievo campioni con archiviazione e definizione automatica delle parole chiave.

c) ***Funzioni di produzione fascicoli (Portale SAA).***
Sono mantenute in efficienza, migliorate e aggiornate le funzioni relative alla produzione dei fascicoli. Il fascicolo costituisce la base di un'attività di monitoraggio avviata su iniziativa dei SAA o su segnalazione scaturita dal sistema MEC, la funzione di apertura del fascicolo è dotata di un'interfaccia che permette il raggruppamento di tutte le azioni e informazioni pertinenti l'azienda/prodotto oggetto del fascicolo nonché la scelta degli utenti coinvolti, ovvero assegnati allo sviluppo dello stesso; la funzione permette di indicare le parole chiave utilizzate dal sistema per ricercare all'interno della sezione documentale del database del portale, tutti documenti che le contengono, e con questi popolare automaticamente il fascicolo appena aperto. La funzione di apertura e assegnazione dei fascicoli è collegata agli strumenti MEC, Agenda, upload documentale e gestione reperti APR.

d) ***Funzioni statistiche e di aggiornamento normativo (Portale SAA).***
Sono mantenute in efficienza, migliorate e aggiornate le funzioni relative alla restituzione dei dati contenuti nel database del portale sia in forma di rapporto testuale che grafico (numero di verbali, numero di analisi, analisi con esiti negativi e positivi, luogo di prelievo campioni, luogo di verbalizzazione, cronologia attività, numero vini monitorati e numero vini sottoposti a controllo; elenco verbali; sanzioni erogate (min-max); contenziosi aperti). Le funzioni statistiche comprendono anche uno strumento di estrazione dei risultati delle analisi per: vitigno/produttore/imbottigliatore.

e) ***Interfaccia di assorbimento e gestione dati provenienti da fonti esterne (Portale SAA).***
E' Sulla scorta delle specifiche emanate dalla Giunta Regionale in relazione al "documento riassuntivo" di cui al comma 2 dell'art. 52 della l.r. 1/2019 potrà essere richiesto lo sviluppo di una nuova funzione del Portale SAA che permetta la costituzione del "documento riassuntivo" di cui all'articolo 52 comma 2 della l.r. 1/2019 e che, tra le altre cose, permetta di gestire i flussi di dati XML delle fatture elettroniche e di oggettivazione e confronto dei dati provenienti dalla GDO (Grande Distribuzione Organizzata). La funzione deve permettere la stampa del documento e prevedere l'auto compilazione con i pertinenti dati presenti a sistema. In mancanza delle specifiche Tali funzionalità

f) ***Interfaccia pubblica portale SAA.***
Il portale è dotato di due interfacce, una privata a esclusivo uso dei SAA e una pubblica, completamente separata dalla prima ove è possibile riversare dati statistici, rapporti, informazioni ritenute di libero accesso. La sezione informativa dell'interfaccia pubblica è mantenuta aggiornata e implementata, a cura del fornitore, con notizie a carattere divulgativo dell'attività dei SAA e informazioni relative alla normativa di settore; le sezioni collegate all'App. Android sono mantenute in efficienza e in sviluppo continuo.

g) ***Sistema di Monitoraggio E-Commerce (MEC)***.
Lo strumento consiste in una banca dati popolata tramite un correlato servizio di monitoraggio delle attività di vendita di prodotti enologici nel web.
L'attività di popolamento della banca dati è articolata in quattro fasi successive: Ricerca, Implementazione, Verifica formale, Esposizione. Al termine delle fasi seguirà il processo decisionale a carico dei SAA.

La fase di ricerca è suddivisa in ulteriori 3 componenti:

ricerca a cadenza mensile dei siti di e-commerce citati (Svinando, Wineverse, Tannico, Vinix, Winetowine e Winezon, Xtrawine, Vinitaly Wine Club, Vino75 e Wineshop), e dei volantini pubblicati sul web delle principali catene della Grande Distribuzione Organizzata (Carrefour, Auchan, Coop, Gigante, Mercatò, In's, Lidl). Tale ricerca potrà essere sostituita e/o alternata con una ricerca di tipo euristico generalizzato al web sia su siti nazionali che internazionali; ricerca euristica su altri siti specializzati e su ditte private esposte sul web al fine di individuare altri siti da inserire nell'elenco dei portali sottoposti a controllo continuo; scopo della ricerca è l'individuazione di offerte o prodotti ritenuti anomali sulla scorta di criteri di selezione definiti dal committente.
ricerca stocastica;
ricerca su segnalazione dei SAA;

La seconda fase, d'implementazione, consiste nell'arricchimento delle informazioni reperite con i necessari dati pertinenti: denominazione, vitigno, casa produttrice, imbottigliatrice; l'elemento viene anche correlato con le eventuali occorrenze presenti in archivio, la fase si conclude con l'archiviazione delle informazioni.

La terza fase consiste nella verifica formale dei dati riportati in etichetta dei prodotti vinari quali: ragione sociale, contrassegno di Stato, Denominazione di Origine, Codice ICQRF;

L'ultima fase, di esposizione del dato acquisito, consiste nella messa a disposizione delle informazioni in formato facilmente leggibile e con funzionalità di raggruppamento, ricerca e comparazione. L'interfaccia di esposizione oltre a permettere l'aggiunta di ulteriori informazioni pertinenti sull'elemento esposto, consente la creazione di un fascicolo, e l'assegnazione del medesimo a un'unità operativa dei SAA.

La funzione dedicata al MEC è mantenuta in efficienza, migliorata e aggiornata. Il database è aggiornato secondo la procedura sopra specificata e tutte le attività ivi previste devono

essere svolte al fine di popolare il database. L'attività relativa alla fase di ricerca deve essere incrementata a non meno di 600 elementi al mese salvo diversi accordi con la struttura appaltante, in particolare l'Ufficio di Coordinamento dei SAA. Nell'attività è compresa la redazione di un manuale sull'utilizzo del sistema, sui parametri di funzionamento e sui criteri elegibili quali discriminanti per la segnalazione da parte del sistema dei prodotti da monitorare.

h) ***App. correlata al sistema MEC.***
Correlata al sistema MEC è presente un App. per smartphone con S.O. Android dedicata all'acquisizione d'immagini elle foto di etichette delle bottiglie di vino che, automaticamente inviate al portale e georeferenziate, vengono successivamente "lavorate" dotandole degli attributi informativi necessari alla verifica formale di cui al precedente punto f) nonché alla loro esposizione, catalogazione e ricerca d'ulteriori dati presenti sul portale. Tale lavorazione fa parte della seconda fase relativa all'attività di popolamento del database citato alla precedente lettera g). L'utilizzo dell'App è consentito a utenti privati solo dietro registrazione sul portale pubblico della piattaforma "portale SAA"; la registrazione consente l'invio ai SAA, da parte dell'utente di segnalazioni informative su prodotti enologici di cui si sospetta la non conformità, nonché l'invio di comunicazioni di riscontro (feedback) e la visualizzazione di notizie inerenti all'attività dei SAA.
L'App. è mantenuta aggiornata, in efficienza, sottoposta a sviluppo continuo e modificata secondo le esigenze rilevate durante il suo utilizzo e tutte le acquisizioni devono essere trattate ed esposte sul portale entro 7 (sette) giorni dal loro invio salvo diversi accordi con il committente. L'App. è correlata alla funzione di composizione dei documenti condivisa al fine di importarne le immagini.

i) ***Funzioni di Agenda***
È mantenuta in efficienza, migliorata e aggiornata la funzione dedicata alla composizione interattiva dell'agenda per la gestione delle attività sul territorio dei SAA.
Gestione vigilanza tramite Aeromobile Pilotaggio Remoto
È mantenuta in efficienza, migliorata e aggiornata la funzione dedicata all'archiviazione dei dati e/o reperti video-fotografici dei voli; al volo è associata una scheda informativa che permette l'inserimento dell'eventuale: piano di volo, verbale e ulteriori informazioni relative all'azienda controllata. È prevista una funzione statistica per la realizzazione di report automatici per la rendicontazione delle attività.

j) ***Funzioni Open Source INTelligence***
È mantenuta in efficienza, migliorata e aggiornata la sezione dedicata all'OSINT, composta da un catalogo di strumenti a uso dei SAA per il reperimento delle informazioni a libero accesso presenti su internet utili ad ampliare l'attività di raccolta informazioni nell'ambito delle attività di monitoraggio e vigilanza.

k) ***Servizi specialistici a supporto dell'Ufficio di coordinamento SAA e dei SAA***
Ulteriori servizi oggetto di affidamento, sono definiti "Servizi specialistici". Tali servizi, atipici, legati alle attività di vigilanza e presidio del territorio e direttamente connessi all'operatività dei SAA e dell'Ufficio di coordinamento sono anche correlati all'implementazione dei disposti di legge di cui all'art. 52 comma 1 lettera f) della l.r. n. 1/2019.Le attività in discorso sono segnalate dall'Ufficio di coordinamento dei SAA, e sono tese all'acquisizione d'informazioni attraverso metodi informatici altamente specialistici e non riproducibili dal personale in organico dei SAA (a titolo di esempio, attività OSINT). Unitamente a tali attività è assicurata ai SAA anche: l'assistenza nell'analisi di reperti informatici acquisiti durante le attività sul territorio; la costruzione di strumenti informatici

ad hoc per lo svolgimento di attività di monitoraggio e vigilanza (a es. predisposizione di strumenti di videosorveglianza a comando remoto); altre attività che comportano un'elevata conoscenza dei sistemi informatici. Ulteriore compito è collegato alla realizzazione di quanto previsto all'art. 52, comma 2, lettera d), e), f) della l.r. 1/2019. Il fornitore dovrà affiancare l'Ufficio di coordinamento nel reperimento, acquisizione, elaborazione e trattamento delle fonti dati, nonché nell'elaborazione di una prassi operativa standardizzata per la composizione e redazione del "documento riassuntivo". Tra i servizi specialistici è compresa l'attività di acquisto presso i siti di eCommerce dei prodotti enologici segnalati dal Committente; il fornitore deve garantire modalità di acquisto del prodotto enologico tali da risultare completamente trasparenti e dimostrabile in tutte le sue parti e, allo stesso tempo, in alcun modo riconducibile alla stazione appaltante; deve inoltre garantire la catena di custodia del prodotto e il mantenimento delle sue caratteristiche organolettiche e chimico fisiche. L'acquisto è effettuato in tripla aliquota (salvo diversa disposizioni da parte dell'ufficio di coordinamento) e tracciato in ogni suo trasferimento, la custodia è garantita nell'imballaggio originale non manomesso in alcun modo e dotato di tutti i documenti di accompagnamento integri e originali, l'immagazzinamento deve avvenire in locale sicuro e idoneo al mantenimento delle caratteristiche organolettiche e chimico fisiche del prodotto e accessibile al committente senza soluzione di continuità e in via autonoma senza preavviso al fornitore. Il valore complessivo dei prodotti acquistati non potrà essere inferiore 500 euro, salvo diversi accordi con l'ufficio di coordinamento SAA. Tutti i costi di acquisto, trasporto, custodia, conservazione, immagazzinamento e assicurazione sono a carico del fornitore.

Ulteriori obiettivi specifici sono costituiti da:

- Innalzamento del livello di sicurezza del sistema di autenticazione;
- Costituzione DB dedicato all'App Android;
- Adeguamento classi php al CLI PDO;
- Adeguamento APP ibrida all'utilizzo delle classi CLI PDO e del nuovo DB;
- Adeguare classi d'accesso;
- Adeguamento portale SAA a colloquiare con database di frontiera sincronizzando i dati in modo sicuro;
- Internazionalizzazione dell'APP;
- Perfezionamento del legame tra documenti presenti nel DB, ivi compreso il MEC (analisi chimico-fisiche, verbali, analisi isotopiche, reperti fotografici);
- Alimentazione DB MEC direttamente dal portale SAA;
- Perfezionamento del sistema di emissioni verbali;
- Perfezionamento moduli ACQUISTI (php modulo esterno fpdf.org);
- ***porting*** del portale su uno spazio web acquistato dal committente al fine di garantirne la funzionalità anche successivamente al termine dell'affidamento**.**

3. Requisiti per l'erogazione dei servizi specialistici richiesti, elementi di carattere essenziale:

Le attività svolte dai SAA di cui al titolo V della l.r. 1/2019 sono svolte da personale in possesso delle funzioni previste all'art.55 del CPP e pertanto, in taluni, casi le informazioni trattate dal contrente durante l'erogazione dei servizi richiesti afferiscono a un ambito caratterizzato da un alto grado di riservatezza relativo alla prevenzione da fenomeni illeciti e al contrasto alle frodi. Inoltre, l'erogazione di taluni servizi specialistici avverrà ai sensi del comma 4 art. 348 del c.p.p., e che in questi casi la prestazione non potrà essere rifiutata dal Fornitore (ex art. 348 c.p.p.), (nella persona contrattualmente individuata*)*, e impegnerà al segreto d'ufficio (ex artt. artt. 326, 357 c.p. e 329 c.p.p.). La materia oggetto d'appalto pone in rilievo il carattere prevalente e prioritario del rapporto

fiduciario tra committente e contrente in conseguenza del quale la stazione appaltante intende definire alcuni elementi essenziali e imprescindibili del contratto:

- per l'espletamento dei servizi in appalto, a esclusione dei servizi di cui al punto 2 lettera f) e g), è richiesto all'operatore economico l'individuazione di una figura di riferimento (di seguito denominata *Referente*), dotata di tutte le competenze del caso e piena autonomia decisionale nell'ambito dell' organizzazione aziendale;
- il referente dovrà:
    - possedere la qualifica di "responsabile di sviluppo" (*Project Manager*), al fine di garantire le necessarie competente e autonomia;
    - essere nominato responsabile della fornitura dall'operatore economico contraente;
    - presentarsi privo di condanne pregresse o in essere, su cui non gravi alcuna interdizione o misura di sicurezza preventiva e che non abbia alcun interesse personale o aziendale nelle attività oggetto di affidamento (ambito agroalimentare);
    - essere in possesso di competenze tecniche in materia di ICT;
    - essere a conoscenza del sistema di rilevazione e controllo della produzione e del commercio delle uve, dei mosti e dei vini istituito in Regione Piemonte con la l.r. 39/80 e, ora con il titolo V della l.r 1/2019;
- essere in possesso d'esperienza almeno decennale:
    - in qualità di Responsabile di sviluppo presso aziende modernamente organizzate in grado di attendere in prima persona alle prestazioni richieste dal presente capitolato a esclusione del mantenimento in operatività del sistema MEC (lettre f) g));
    - nella gestione/progettazione/sviluppo di sistemi *software* gestionali (contabili/fiscali) nonché la conoscenza dei principi contabili/gestionali (flussi XBRL, dichiarazioni telematiche, fatturazione elettronica) e la conoscenza dell'organizzazione dei flussi aziendali;
    - attività di *audit* su software di terze parti (al fine di accertare competenze su software sviluppati da terzi):
    - nell'utilizzo delle principali tecniche di analisi dei dati web di libero accesso, ivi compresa l'analisi del codice di sviluppo legalmente reperibile;
    - amministratore di almeno un sito internet con qualifiche di sicurezza **di livello NON inferiori ad A** testate con strumenti quali: **https://observatory.mozilla.org**, e secondariamente https://securityheaders.com/, **https://www.ssllabs.com/.**

4. Requisiti prestazionali del Portale SAA richiesti; elementi di carattere essenziale.

Per il mantenimento in efficienza, implementazione e ulteriore sviluppo del Portale SAA è richiesta l'elaborazione di soluzioni software originali e sviluppate *ad hoc* al di fuori di ambienti di sviluppo standardizzati riconducibili alla categoria CMS (Content Management System: sistema organizzato e standardizzato di processi e tecnologie a supporto della raccolta, della gestione e della pubblicazione di informazioni). Possono invece essere utilizzati *tools* di sviluppo qualora questi non vincolino le scelte progettuali richieste dalle caratteristiche del servizio in modo tale da impedire il raggiungimento del risultato atteso. Il nuovo codice deve essere sviluppato in aderenza al documento ANAC, approvato con propria Delibera numero 950 del 13 settembre 2017 - Linee guida n. 8 "*Ricorso a procedure negoziate senza previa pubblicazione di un bando nel caso di forniture e servizi ritenuti infungibili*".

Le tecnologie utilizzate devono essere *Open source*, e i *plug-in* utilizzati devono essere di libero utilizzo. Lo sviluppo del codice non deve comportare alcuna spesa di licenza software a esclusione dei costi legati ai servizi server.
Il codice sorgente dovrà essere scritto secondo le *best practices* presenti nel manuale ufficiale PHP (PHP.net), aderendo agli standard di codifica individuati dal php_fig.org al fine di rendere l'interpretazione del codice il più accessibile possibile a diversi autori e programmatori. La stessa logica di utilizzo di pratiche di sviluppo condivise dalle comunità di progettazione più rappresentative è da applicarsi anche verso gli altri linguaggi di programmazione utilizzati (HTML5, Javascript, etc). Si richiede lo sviluppo di codice che prosegua con l'architettura già impostata *three-tier*: INTERFACCIA, LOGICA BUSINESS, DATI), che NON utilizzi il metodo GET per cambiare lo stato delle informazioni sul server e che sia:

- commentato;
- autoesplicativo;
- modulare;
- impostato secondo una metodologia di sviluppo di tipo iterativo (a spirale), così da consentire un costante coinvolgimento del fornitore e premettere al progetto di acquisirne le necessità;
- i moduli o componenti che costituiscono il software devono essere descritti in modo tale che, per ciascun modulo, venga specificato il contenuto informativo richiesto in ingresso e quello atteso in uscita, non tralasciando le specifiche relative al tipo di tracciato dati e ai tipi di formato utilizzati così come suggerito dalle linee guida n. 8 ANAC al punto 2.4 lettera c).

Per quanto riguarda il *server* di appoggio, le spese di mantenimento sono a totale carico del Fornitore, il *server* deve garantire i più alti *standard* di sicurezza e velocità ed essere collocato all'interno della UE; è esclusa la possibilità di trasferimento, anche temporaneo al di fuori degli spazi comunitari.

Le prestazioni relative alla sicurezza del portale saranno testate a cadenza mensile per la verifica dell'adozione delle corrette pratiche di sicurezza nella configurazione del sito web attraverso strumenti *on-line* quali **https://observatory.mozilla.org**, e secondariamente **https://securityheaders.com/**, **https://www.ssllabs.com/**, il Portale dovrà essere, tra le altre cose, protetto da attacchi informatici generici e di sottrazione di sessione d'autenticazione. Il livello di protezione richiesto è **almeno di grado B** (scala observatory.mozilla). L'accesso alle cartelle del Portale SAA deve essere sottoposto ad autenticazione lato server tramite credenziali di autenticazione e lato client tramite piattaforma di autenticazione fisico-logica proprietaria. Ulteriori specifiche di sicurezza potranno essere richieste e concordate durante lo svolgimento della commessa.

I costi correlati al server che ospita il portale e delle opzioni necessarie a garantire più alti livelli di sicurezza, le migliori prestazioni in termini di stabilità e velocità, il backup periodico e quant'altro necessario al mantenimento del sito efficiente ed efficace, sono a carico del contraente fino al termine della garanzia del software (clausola 25 TITOLO II).

5. Attività di progettazione cooperativa, assistenza e formazione;

Relativamente ai servizi di sviluppo, manutenzione evolutiva e implementazione di nuovi servizi del software e dell'app, sono previste attività di progettazione, assistenza e formazione.

a) ***Progettazione cooperativa:***
È richiesto che l'attività di manutenzione e sviluppo del nuovo codice relativo al portale SAA avvenga attraverso un processo di progettazione cooperativa con il Committente al fine di

concordare le soluzioni applicative e le routine applicative più aderenti agli scopi del Portale SAA. A tale scopo devono essere svolti incontri di confronto, a cadenza mensile, tra il Referente e il responsabile del progetto presso la sede del Committente.
Le decisioni e gli orientamenti assunti durante gli incontri dedicati alla progettazione cooperativa costituiscono elementi integranti le caratteristiche del servizio richiesto, ovvero la loro corretta implementazione costituisce elemento di verifica durante il collaudo del rilascio della versione finale del prodotto.

b) ***Assistenza:***

L'assistenza richiesta si articola in due principali rami, assistenza all'utenza (servizi SAA), e assistenza al Committente (Direzione Agricoltura – Settore A1706A Servizi di sviluppo e controlli in agricoltura - Ufficio di Coordinamento SAA); nel secondo caso l'attività di assistenza all'utilizzo del portale o di risoluzione di errori bloccanti è erogata e ricompresa nella precedete lettera a) progettazione cooperativa.

Per quanto riguarda l'assistenza agli utenti è necessario che essa sia articolata su due livelli con le specificate prerogative:

1. Assistenza via *e.mail*. L'assistenza è continua per 8 ore al giorno (9:00–12:30, 13:00-17:30) durante i feriali, per tutto il periodo del contratto, ed è così articolata:
    - *errore bloccante*: il Fornitore richiede all'utente tutti gli elementi necessari e apre un *ticket* di richiesta, successivamente interviene sul programma modificandone, se necessario, anche il codice di programmazione. Il *ticket* è inviato per conoscenza anche alla Direzione Agricoltura – Ufficio di Coordinamento SAA e all'utente assistito;
    - *richiesta di aiuto per l'utilizzo del Portale SAA*: fornisce le istruzioni via e-mail e se necessario integra la FAQ presenti nella home del portale;
    - *richiesta modifica* funzionalità: acquisisce e inoltra la richiesta alla Direzione Agricoltura – Ufficio di Coordinamento SAA unitamente a una prima valutazione di fattibilità e costi.
2. Assistenza via telefono o con desktop remoto: l'assistenza è attivata tramite *ticket* di richiesta ed è gestita secondo la seguente casistica:
    - *Errore bloccante* causato da bug di programma o da un errata interpretazione delle specifiche: il Fornitore interviene in maniera risolutiva (tale da ripristinare le corrette funzionalità del sistema), entro le 24 ore successive alla notifica, tutti i giorni della settimana (feriali e festivi) per tutto il periodo del contratto;
    - *Errore bloccante* non dipendente da bug di programma: il Fornitore interviene (in maniera risolutiva nel limite delle responsabilità o corresponsabilità di malfunzionamento riconducibili al software sviluppato), entro gli 8 giorni successivi alla notifica, tutti i giorni della settimana (festivi e feriali), per tutta la durata del contratto.

c) ***Formazione***:

La formazione al Committente è erogata e ricompresa in quanto previsto nella precedente lettera a) "Progettazione cooperativa". La formazione per gli utenti è effettuata tramite l'erogazione di un evento formativo della durata di mezza giornata (almeno 4 ore), nel corso del 2019 presso la sede del Committente. La produzione del materiale esplicativo è a cura del Fornitore, è invece a cura del Committente la riproduzione di detto materiale per gli utenti finali. La formazione è erogata dal Referente.

6. Servizi specialistici e attività che non comprendono lo sviluppo di software

I servizi specialistici e a tutte quelle attività che non comportano lo sviluppo di software o di applicazioni Android (definite e regolate tramite "Progettazione cooperativa"), sono disposte e/o concordate con il contraente a seconda della loro natura, dall'ufficio di coordinamento attraverso "Disposizioni operative". Tali disposizioni emanate nell'alveo di legittimità contrattuale, costituiscono elementi integranti le caratteristiche del servizio richiesto, ovvero la loro corretta implementazione costituisce elemento di verifica per l'accettazione delle attività svolte.

7. Obblighi di presenza in sede – trasferte.

Le attività specialistiche comportano la presenza del *Referente* presso la sede regionale ubicata in Corso Stati Uniti, 21 - 10128 Torino, (salvo diverse disposizioni concordate con l'Ufficio di coordinamento dei SAA), per almeno un giorno a settimana in orario di compresenza con il personale d'ufficio nonché l'esecuzione di trasferte su tutto il territorio regionale, anche in orari notturni. Non sono previsti rimborsi spese né di trasferta. Le attività specialistiche di cui alla lettera k) del punto 2 del presente documento, concordate direttamente con l'Ufficio di coordinamento SAA, prevedono la reperibilità del fornitore 24 ore su 24 per 7 giorni su 7 (feriali e festivi).

TITOLO II
ELEMENTI ESSENZIALI DEL CONTRATTO D'AFFIDAMENTO DEL SERVIZIO

8. Oggetto del contratto

Acquisizione di *"Servizi specialistici di supporto anche informatico alle attività di vigilanza e controllo dei SAA"* di cui al Titolo V "Contrasto alle frodi" della l.r. n. 1 del 22 gennaio 2019.

La realizzazione del software e l'erogazione dei servizi specialistici avvengono esclusivamente secondo le modalità indicate nel presente documento. L'erogazione di taluni servizi specialistici avverrà ai sensi del comma 4 art. 348 del c.c.p., in questi casi la prestazione non potrà essere rifiutata dal fornitore (ex art. 348 c.c.p.), (nella persona contrattualmente individuata e definita *Referente,* e impegnerà al segreto d'ufficio (ex artt. artt. 326, 357 c.p. e 329 c.p.p.).

9. Modalità di stipulazione del contratto

L'incarico è formalizzato mediante scrittura privata in forma elettronica, ai sensi del D.lgs. 50/2016 e s.m.i., e dell'art. 17 della legge regionale n. 23 del 2008, così come disposto dall'art 6 comma 6 del Decreto legge n. 145 del 23.11.13.

10.Divieto di subappalto e cessione del contratto

Sono vietati il subappalto e la cessione del contratto, sia totale che parziale, pena l'immediata risoluzione del contratto senza alcun onere a carico della stazione appaltante.

11. Responsabilità del Fornitore

Il Fornitore è responsabile della conformità del software realizzato alle specifiche tecniche e funzionali (c.d. **obbligazione di risultato**), come precisato nel presente documento.

Il Fornitore si impegna a operare con professionalità e diligenza e in conformità con le clausole di riservatezza e di *privacy* nell'esecuzione della propria attività inerenti al Portale SAA e i servizi specialistici. Nel caso delle attività legate al sistema MEC, il Fornitore si impegna a mettere a disposizione del Committente le necessarie risorse umane e tecniche, garantendo la competenza nonché la professionalità propria e dei propri dipendenti e collaboratori al fine di sviluppare software con buone caratteristiche qualitative.

Relativamente all'erogazione dei "Servizi specialistici" e di ogni altra attività al di fuori di quanto richiesto relativamente alle funzionalità del sistema MEC, il Fornitore si impegna a operare esclusivamente tramite il *Referente* individuato in sede d'affidamento, senza capacità di demandare ad altri alcuna mansione.

12. Clausola di sicurezza relativa al Portale

Il contraente si impegna a garantire elevati *standard* di sicurezza del portale, in particolare il mantenimento delle qualifiche di sicurezza del sito **a livello B** o superiore rilevati con strumenti quali: **https://observatory.mozilla.org**, e secondariamente https://securityheaders.com/, **https://www.ssllabs.com/** .

Il committente può procedere a verifiche relative alla sicurezza, anche a cadenza mensile, in proprio o attraverso terzi specializzati al fine di accertare il livello di vulnerabilità.; in caso di difformità assegnerà al Fornitore, mediante comunicazione scritta, un termine massimo di 5 (cinque) giorni per far cessare la violazione. Decorso inutilmente tale termine senza che il Fornitore abbia

cessato la condotta lesiva della sicurezza del sito e delle informazioni ivi contenute, **il Committente potrà dichiarare risolto il contratto ai sensi dell'art. 1456 c.c. con comunicazione scritta al Fornitore**, fatti salvi gli ulteriori diritti e azioni spettanti al Committente in base al presente Contratto e alle norme applicabili. In caso di risoluzione del contratto, il Fornitore non avrà diritto ad alcun compenso, indennità o risarcimento per l'anticipato scioglimento del rapporto.

13. Clausole di riservatezza

A eccezione del sistema MEC, è fatto assoluto divieto di condivisione di dati e/o informazioni di qualsivoglia natura.

Il Fornitore si impegna, per sé e i suoi dipendenti, collaboratori, consulenti e subfornitori a mantenere la massima riservatezza in merito alle informazioni ai dati e relativi al servizio affidato e al Committente, di cui verrà a conoscenza, a qualsiasi titolo, in relazione all'esecuzione del presente Contratto. Si considera rientrante nei suddetti dati e informazioni anche qualsiasi notizia attinente all'attività svolta dal Committente, ai suoi beni strumentali mobili e immobili, e al suo personale di ruolo o meno, acquisita durante lo svolgimento dei Servizi.

L'obbligo di riservatezza riguarda, in particolare, le informazioni sensibili acquisite nel corso dello svolgimento delle prestazioni previste in contratto.

Il Fornitore si impegna a:

- garantire che le informazioni e i dati e acquisiti siano utilizzati esclusivamente nell'interesse del Committente per le finalità inerenti all'esecuzione del contratto;
- garantire che nessuna di tali informazioni sia diffusa verso soggetti terzi estranei al rapporto contrattuale, per alcun motivo, salvo in caso di preventiva autorizzazione scritta del Committente;
- garantire che la diffusione delle informazioni all'interno della sua azienda sia limitata esclusivamente ai soggetti coinvolti nell'esecuzione del contratto;
- fornire tempestivamente, a richiesta del Committente, l'elenco dei documenti, informazioni e dati acquisiti in qualunque modo durante l'esecuzione del contratto;
- comunicare tempestivamente, su richiesta del Committente, l'elenco del personale che, direttamente o indirettamente, svolge mansioni che comportano l'accesso alle informazioni sensibili;
- consentire al Committente di verificare, in qualsiasi momento e dietro semplice richiesta, anche mediante accessi e ispezioni presso la sede del Fornitore, che i dati e le informazioni siano gestiti in conformità alle disposizioni del presente contratto;
- distruggere i documenti, le informazioni e i dati di cui sopra quando non sono più necessari per l'esecuzione del contratto e, in ogni caso, dopo la cessazione del rapporto contrattuale, dandone tempestiva comunicazione per iscritto al Committente.

Il presente obbligo di riservatezza vincolerà il Fornitore, i suoi dipendenti, collaboratori, consulenti e subfornitori, per tutta la durata del contratto e per i 5 (cinque) anni successivi alla data della sua cessazione, per qualunque causa essa sia avvenuta, salvo che la comunicazione dei dati sensibili sia prescritta per ordine dell'Autorità giudiziaria o di altre Autorità competenti. In tal caso, il Fornitore sarà tenuto a darne preventiva notizia al Committente, in modo da evitare o limitare eventuali pregiudizi all'attività di quest'ultimo.

In caso di violazione dell'obbligo di riservatezza, il Committente assegnerà al Fornitore, mediante comunicazione scritta, un termine massimo di 15 (quindici) giorni per far cessare la violazione. Decorso inutilmente tale termine senza che il Fornitore abbia cessato la condotta lesiva della riservatezza delle informazioni, **il Committente potrà dichiarare risolto il contratto ai sensi dell'art.**

1456 c.c. con comunicazione scritta al Fornitore, fatti salvi gli ulteriori diritti e azioni spettanti al Committente in base al presente Contratto e alle norme applicabili. In caso di risoluzione del contratto, il Fornitore non avrà diritto ad alcun compenso, indennità o risarcimento per l'anticipato scioglimento del rapporto.

14.Sede di esecuzione dei servizi specialistici oggetto di appalto

Le attività specialistiche comportano la presenza del Fornitore nella figura del *Referente* responsabile di progetto presso la sede regionale ubicata in Corso Stati Uniti, 21 - 10128 Torino, per almeno un giorni a settimana in orario di compresenza con il personale d'ufficio, salvo diversi accordi con la struttura appaltante, in particolare l'Ufficio di Coordinamento dei SAA. E' richiesta la disponibilità del *Referente* a effettuare trasferte su tutto il territorio regionale, anche in orari notturni. **Le attività concordate direttamente con l'ufficio di coordinamento SAA, prevedono la reperibilità del fornitore 24 ore su 24 per 7 giorni su 7 (feriali e festivi).**

In caso d'inadempienza rispetto a quanto richiesto tramite disposizioni operative, il Committente assegnerà al Fornitore, mediante comunicazione scritta, un termine massimo di 15 (quindici) giorni per far cessare la violazione. Decorso inutilmente tale termine senza che il Fornitore abbia cessato la condotta lesiva della riservatezza delle informazioni, **il Committente potrà dichiarare risolto il contratto ai sensi dell'art. 1456 c.c. con comunicazione scritta al Fornitore**, fatti salvi gli ulteriori diritti e azioni spettanti al Committente in base al presente Contratto e alle norme applicabili. In caso di risoluzione del contratto, il Fornitore non avrà diritto ad alcun compenso, indennità o risarcimento per l'anticipato scioglimento del rapporto.

15.Durata dell'incarico e termini di consegna

L'incarico ha durata biennale a decorrere dalla data di stipulazione del contratto e termina nel dicembre 2022.
Le scadenze per l'erogazione dei servizi oggetto di appalto e delle singole attività sono concordate con la stazione appaltante e, in particolare, con l'Ufficio di coordinamento in sede di progettazione cooperativa (punto 5 Titolo I), o contenute nelle disposizioni operative di cui al punto 6 titolo I del presente documento. I termini ivi definiti divengono elementi essenziali del contratto.~~.~~

16.Variazione nei tempi previsti relativi alle consegne intermedie del software

Nel caso in cui l'attività di sviluppo del software non possa svolgersi secondo i termini concordati in sede di programmazione cooperativa ~~indicati nel Piano di Lavoro~~ a causa di comprovate e imprevedibili ragioni tecniche di carattere oggettivo, il Fornitore è tenuto a comunicare tempestivamente al Committente i motivi e l'entità del ritardo. L'entità del ritardo deve comunque essere congrua rispetto ai motivi addotti.
Il Committente ha diritto di recedere dal contratto nel caso in cui il ritardo annunciato dal Fornitore sia superiore a 15 giorni.
Qualora il Committente non si avvalga della facoltà di recesso, le parti procedono alla riformulazione dei nuovi termini di consegna delle versioni intermedie da parte del Fornitore.

17. Importo a base di affidamento

Euro 77.000,00 più I.V.A. suddivisi in due annualità:

per il 2021, euro 38.500 più IVA;

per il 2022, euro 38.500 più IVA.

18.Modalità di erogazione del compenso

La liquidazione del corrispettivo ha luogo in quattro (4) *tranche* semestrali a Stato Avanzamento Lavori (SAL) coincidenti con l'avanzamento delle attività svolte del software richiesto e delle attività relative ai "servizi specialistici". La liquidazione avviene dietro emissione di relativa fattura elettronica. Se tra le attività previste e concordate con la stazione appaltante in sede di progettazione cooperativa, figura lo sviluppo o l'implementazione o la manutenzione evolutiva di un software o di un applicazione la fattura, corredata di una relazione di accompagnamento, dovrà essere emessa successivamente alla procedura di verifica e accettazione del software specificate ai successivi punti del presente Titolo II. Per quanto attiene al software la relazione dovrà essere analitica e comprensiva del dettaglio di costo; per quanto riguardano i "servizi specialistici", la relazione dovrà riguardare gli ambiti dell'attività svolta e, per quanto riguarda i servizi resi relativamente alle operazioni di controllo dei prodotti enologici venduti nel mercato elettronico, dovrà esplicitare analiticamente tutti gli acquisti effettuati e i costi sostenuti a diverso titolo per l'acquisizione, trasporto, stoccaggio, conservazione, vigilanza del prodotto acquistato e quant'altro pertinente. Il termine del pagamento è di 30 giorni a partire dalla data di ricevimento della fattura. Il pagamento è subordinato all'esito regolare del DURC (Documento Unico di Regolarità Contributiva), che sarà richiesto dalla stazione appaltante alla ricezione della fattura.

L'importo richiedibile dal fornitore alla prima *tranche* (primo SAL) non può essere superiore al 50% dell'importo complessivo dell'affidamento.

19.Penalità

Nel caso di mancato rispetto del termine indicato per la consegna di software o dei servizi specificati al punto 2 Titolo I del presente documento è applicata una penale commisurata all'importo contrattuale: essa è calcolata come una percentuale dell'importo contrattuale pari a un terzo del rapporto tra i giorni di ritardo e la durata, espressa in giorni, prevista per l'esecuzione della prestazione del fornitore. Per il calcolo dei giorni di ritardo il termine iniziale coincide con il giorno in cui il servizio avrebbe dovuto essere svolto (o a disposizione del committente se trattasi di software), per l'espletamento della verifica di conformità.

Nell'ipotesi in cui il software non superi positivamente la verifica, la consegna si considera come non avvenuta; in questo caso, ai fini del calcolo del ritardo per la penale, non si considera il periodo intercorso tra la messa a disposizione del software per l'espletamento della verifica di conformità e la comunicazione, da parte del committente, del mancato superamento dello stesso.

Nell'ipotesi in cui l'attività richiesta non venga erogata con le modalità richieste e specificate in sede di programmazione cooperativa o contenute nelle disposizioni operative, l'attività è considerata non conforme e si considera come non avvenuta; in questo caso, ai fini del calcolo del ritardo per la penale, non si considera il periodo intercorso per la verifica di conformità dell'attività e la comunicazione, da parte del committente, del mancato superamento dello stesso.

L'esito negativo di ciascuna verifica comporta, comunque, l'applicazione di una penale pari al 3% dell'importo contrattuale, che potrà essere riassorbita dalla penale complessiva maturata a causa del ritardo (ove la penale complessiva sia maggiore delle penali maturate a causa di mancata accettazione).

Il committente ha facoltà di procedere alla risoluzione del contratto qualora la penale raggiunga un importo pari al 10% dell'importo contrattuale.

L'ammontare della penale, in ogni caso, non può essere superiore al 30% del corrispettivo pattuito per il contratto.

In caso di mancata esecuzione dei servizi entro i termini stabiliti, l'Amministrazione può dichiarare decaduta la Ditta affidataria e la stessa non potrà avanzare alcuna pretesa.

20.Richieste informazioni, verifiche in corso d'opera e ispezioni

In qualsiasi momento dello svolgimento del rapporto, il Committente potrà richiedere al Fornitore la comunicazione di dati e informazioni relativi all'andamento dell'attività e dei servizi a lui affidati e, con un congruo termine di preavviso, la presentazione di una relazione sull'andamento e sui livelli qualitativi del servizio. Il compenso per lo svolgimento di tale attività è già compreso nel corrispettivo pattuito tra le Parti per il contratto.

Il Committente ha diritto di effettuare, anche tramite un proprio incaricato di fiducia, la verifica della corretta esecuzione dell'attività di sviluppo da parte del Fornitore presso la sede operativa di quest'ultimo. A tal fine il committente è tenuto a preannunciare la visita al fornitore tramite mail, con 1 giorno di anticipo. In ogni caso il diritto di verifica non può esercitarsi più di 2 volte al mese.

Il Fornitore è tenuto a prestare la massima collaborazione affinché il personale incaricato dal Committente possa espletare nel modo più efficiente le verifiche e le ispezioni suddette; in particolare, sarà obbligato a:

- fornire qualsiasi informazione in merito alle modalità di svolgimento dei servizi;
- esibire e fornire copia di tutta la documentazione attinente alla prestazione dei servizi; qualora non fosse possibile esibire o produrre copia della documentazione richiesta nel corso della verifica, il Fornitore dovrà soddisfare le richieste del Committente al più tardi entro 10 (dieci) giorni dalla conclusione delle operazioni di verifica;
- consentire al Committente di formulare domande al personale del Fornitore addetto allo svolgimento dei servizi. Le verifiche e le ispezioni saranno condotte in contraddittorio tra le parti, le quali provvederanno a redigere un verbale delle operazioni compiute.

Qualora il Fornitore:

(i) non trasmetta i dati e le informazioni richieste;
(ii) non predisponga la relazione sull'andamento e sui livelli di qualità del servizio senza indicare validi motivi;
(iii) non permetta al Committente di espletare le verifiche e le ispezioni

il Committente assegnerà al Fornitore un termine massimo di 30 (trenta), giorni per adempiere gli obblighi di informazione. **Decorso inutilmente il termine assegnato, il Committente avrà diritto di dichiarare la risoluzione del contratto ai sensi dell'art. 1456 c.c., con comunicazione scritta al Fornitore. Il Fornitore, invece, non avrà diritto ad alcun compenso, indennità o risarcimento per l'anticipato scioglimento del rapporto**.

Se dalla verifica emergono difformità nell'attività di sviluppo del software e dei servizi richiesti rispetto a quanto concordato in sede di progettazione cooperativa o definito nelle disposizioni operative impartite dalla stazione appaltante per tramite dell'ufficio di coordinamento dei SAA, o ancora risulti il mancato rispetto delle regole dell'arte, il Committente comunica per iscritto, tramite *e-mail*, al Fornitore tali circostanze e gli intima di provvedere all'adeguamento rispetto a quanto concordato e/o definito entro il termine di 30 (trenta), giorni di calendario, pena la risoluzione di diritto del contratto ai sensi dell'art. 1662 cod. civ.

Allo scadere del termine assegnato, nel caso in cui il Committente riscontri, a seguito di un ulteriore controllo, il persistere dell'inadempimento, il contratto si intenderà risolto di diritto.

21.Modalità di consegna del software e di relazione sulle altre attività

Il Fornitore si impegna a consegnare al Committente il software sviluppato: in particolare egli è tenuto a installare e configurare il software nelle apparecchiature hardware del server utilizzato per l'erogazione del servizio in *cloud*, in modo che il software sia "pronto all'uso" entro i termini pattuiti.

Il Fornitore, unitamente al software di cui al precedente comma, fornisce al Committente tutte le credenziali necessarie (amministratore) a operare sullo spazio web ove risiede la piattaforma "Portale SAA". Il Committente può utilizzare tali credenziali al solo fine di effettuare il *porting* su altro server o a modificare, previa comunicazione al Fornitore, i parametri dei servizi web qualora aggiornamenti dei medesimi abbiano comportato malfunzionamenti del software sviluppato.

Il Fornitore non è tenuto a effettuare ulteriori configurazioni e/o installazioni rispetto a quelle iniziali, salvo che esse siano rese necessarie da difetti del software o da errori nelle operazioni iniziali.

Il Fornitore si obbliga altresì a consegnare, contestualmente al software, i manuali operativi per l'installazione, la configurazione e l'utilizzo del software, e la relativa documentazione tecnica esplicativa.

Il Fornitore si impegna altresì consegnare al Committente una relazione sulle attività svolte e richieste tramite le disposizioni operative impartite dal Committente per tramite dell'ufficio di coordinamento dei SAA. La relazione, consegnata entro e non oltre 10 giorni dal termine dell'attività, specifica modalità operative, strumenti, personale impiegato, luoghi e tempi di svolgimento nonché riporta i risultati ottenuti. Ulteriori modalità di relazione sono concordate con l'ufficio di Coordinamento dei SAA.

22.Verifica rilascio versioni intermedie e finale del software.

Il Fornitore è tenuto a eseguire la configurazione del software necessario alla fruizione della piattaforma "Portale SAA" sulle apparecchiature hardware del Committente affinché questi possa espletare le operazioni di verifica del software.

La procedura di verifica è volta a testare la rispondenza del software ai risultati attesi ed espressi nel presente documento; la verifica si svolge tramite l'analisi del codice sviluppato e la simulazione delle attività che gli utenti sono chiamati a effettuare attraverso il portale, nonché l'accertamento della presenza delle funzionalità, delle caratteristiche richieste e l'adempimento dei compiti oggetto di affidamento. Le difformità sono rilevate ai sensi del presente documento

Per la verifica delle versioni sia intermedie che finali il Committente ha l'obbligo di utilizzare la Procedura di Accettazione specificata nel presente documento e di segnalare per iscritto, tramite email al Fornitore, eventuali fallimenti di uno o più test della Procedura entro e non oltre 10 giorni lavorativi dal completamento delle operazioni di configurazione eseguite per consentire la verifica. La segnalazione dei fallimenti riscontrati determina il mancato superamento della verifica e implica la mancata accettazione della versione software intermedia, salvo in caso di accettazione con riserva da parte del Committente.

Nel caso di esito negativo della verifica, il Fornitore è tenuto a eliminare i difetti riscontrati entro 10 giorni lavorativi. Il Committente, ricevuto il software, procede a una nuova verifica. Il contratto si intenderà risolto di diritto qualora il software dovesse nuovamente presentare difetti, malfunzionamenti o errori, a seguito della segnalazione dei nuovi fallimenti da parte del Committente.

Trascorso il termine di cui al comma precedente senza che al Fornitore sia pervenuta alcuna contestazione da parte del Committente, il software si intende accettato ai sensi dell'art. 1665, comma 3, cod. civ. e il Fornitore matura il diritto al pagamento del corrispettivo.

Nel caso di rilascio di versione intermedie e/o parziali del software il Committente procede alla loro verifica. In ogni caso né le verifiche eseguite, né gli acconti corrisposti valgono quale accettazione parziale del software consegnato per la verifica finale.

Il Committente che durante la procedura di Accettazione ha considerato adeguati comportamenti del software difformi da quanto atteso in relazione alle specifiche richieste nel presente documento, non potrà far valere per tale difformità la garanzia di cui alla clausola 24.

Il Committente ha la facoltà di "accettare con riserva" i malfunzionamenti del software che ritiene siano tali da non impedire l'accettazione finale ma che, tuttavia, esige siano corretti dal Fornitore secondo le modalità fissate nella clausola 25, "Garanzia (manutenzione)".

23.Verifica delle attività che non comprendono lo sviluppo del *software*.

La procedura di verifica è volta a rilevare la corrispondenza tra le attività richieste e quelle svolte, sia sotto il profilo dei risultati ottenuti che dei tempi, strumenti e modalità di intervento, ovvero accertare la diligenza nell'effettuazione delle attività richieste e l'aderenza alle disposizioni operative impartite.

Il Committente ha l'obbligo di utilizzare la Procedura di Accettazione specificata nel presente documento e di segnalare per iscritto, tramite email al Fornitore, eventuali osservazioni in merito all'attività svolta rilevandone le difformità lamentate entro e non oltre 10 giorni lavorativi dal completamento del ricevimento della relazione sull'attività. La segnalazione delle difformità determina il mancato superamento della verifica e implica la mancata accettazione della versione software intermedia, salvo in caso di accettazione con riserva da parte del Committente.

Trascorso il termine di cui al comma precedente senza che al Fornitore sia pervenuta alcuna contestazione da parte del Committente, l'attività si intende accettato ai sensi dell'art. 1665, comma 3, cod. civ. e il Fornitore matura il diritto al pagamento del corrispettivo.

Nel caso di esito negativo della verifica, il Fornitore è tenuto a porre rimedio alle mancanze riscontrate entro 10 giorni lavorativi e a integrare la relazione a suo tempo presentata. Il Committente, ricevuta la relazione procede a una nuova verifica. Il contratto si intenderà risolto di diritto qualora l'attività svolta dovesse nuovamente risultare difforme da quanto richiesto da parte del Committente.

Il Committente ha la facoltà di "accettare con riserva" la seconda relazione qualora le difformità rilevate siano tali da non inficiare l'esito dell'attività richiesta. Tuttavia il contratto s'intenderà risolto di diritto al superamento delle tre (3) relazioni accettate con riserva.

Il Committente che durante la procedura di Accettazione ha considerato adeguato lo svolgimento dell'attività richiesta anche se difforme da quanto definito delle disposizioni operative non potrà più far valere per tale difformità.

24.Procedura di Accettazione del *software*.

La procedura di Accettazione/collaudo del software sviluppato, salvo diversi accordi, avviene presso la sede del Committente e con la sua strumentazione hardware alla presenza del fornitore. Ambiente software utilizzato: Windows 10/7; Browser utilizzato: Firefox, Chrome, Ie, ultime versioni; Connessione internet utilizzata: banda larga, chiavetta 4G.

25.Procedura di Accettazione delle attività diverse dallo sviluppo *software*.

La procedura di Accettazione delle attività svolte consiste nella verifica delle modalità operative adottate dal contraente per lo svolgimento delle attività richieste tramite disposizioni operative nonché degli strumenti del personale impiegato dei luoghi e dei tempi impiegati e dei risultati ottenuti. La verifica è effettuata anche sulla scorta della relazione presentata al termine delle attività richieste. Il Committente, in caso di difformità, può convocare in contraddittorio il contraente per un confronto verbale; in tal caso il termine per la presentazione delle segnalazioni di cui al punto 23 è differito di ulteriori 10 giorni.

26.Garanzia e manutenzione del software rilasciato.

Il Fornitore si impegna a garantire, per la durata di anni uno (1) dall'accettazione del software, gli interventi di manutenzione e/o di modifica necessari al fine di eliminare le eventuali difformità del software sviluppato rispetto alle specifiche tecniche e funzionali concordate nel "Programma" riscontrate successivamente alla conclusione del contratto. Egli, inoltre, si obbliga a eliminare i comportamenti del software che dovessero rivelarsi "non accettabili", e a seguito della ripetizione della Procedura di Accettazione, effettuata in occasione di una revisione del software a patto che quest'ultimo non sia stato in alcun modo modificato da terzi.

L'intervento del Fornitore volto alla constatazione dell'esistenza del problema segnalato dal Committente dovrà essere effettuato entro 8 ore lavorative del giorno successivo alla segnalazione.

Le operazioni di manutenzione devono concludersi in un termine congruo, avuto riguardo alla complessità del software, alla gravità del difetto e alle difficoltà di intervento. Tali operazioni sono svolte a spese del Fornitore ai sensi dell'art. 1668 cod. civ.

La revisione (o *patch*) del software si intende accettata se non presenta più i difetti denunciati e se supera con esito positivo tutti i test previsti dalla Procedura di Accettazione di cui al Piano di Lavoro. Tale revisione (o tale *patch*) del software, volta all'eliminazione dei difetti non deve introdurre nuovi errori e/o difetti (regressioni), né creare ulteriori malfunzionamenti; inoltre il Fornitore deve assicurare la conversione dei dati caricati con il vecchio formato in quello nuovo.

La manutenzione del software verrà effettuata mediante rilascio della nuova revisione, o della patch, in via telematica (da remoto), sul server ove è ospitata la piattaforma software; il Fornitore informa il Committente delle operazioni di manutenzione.
La garanzia cui è tenuto il Fornitore ai sensi della presente clausola è esclusa in caso di uso del software non conforme alle istruzioni indicate nel manuale d'uso consegnato al Committente.

27.Titolarità del codice sorgente

Il Fornitore si impegna a consegnare al Committente, oltre al software in forma di codice oggetto, anche il codice sorgente dell'applicazione e la relativa documentazione tecnica.

Il Committente consegue il diritto di modificare ed estendere il software secondo le proprie esigenze; inoltre il Committente acquisisce ogni diritto connesso allo sfruttamento commerciale del software sviluppato.

Il Fornitore si impegna altresì a risarcire e tenere indenne il Committente da qualsivoglia azione che dovesse essere intrapresa da terzi in relazione a presunti diritti vantati sul software, nonché a intervenire nei giudizi civili e/o penali eventualmente promossi da terzi, anticipando spese e oneri che il Committente si trovasse a dover affrontare in relazione a detti giudizi.

28.Servizi specialistici

Il Fornitore è tenuto a prestare la propria opera e assolvere a quanto richiesto per l'espletamento dei compiti previsti alla citata lettera l) "*Servizi specialistici a supporto dell'Ufficio di coordinamento SAA e dei SAA*" dietro specifica richiesta del Committente emanate attraverso le "disposizioni operative". Il mancato assolvimento di quanto richiesto entro i termini di volta in volta indicati e secondo modalità difformi da quanto richiesto, è causa di immediata rescissione del contratto.

TITOLO III
INFORMAZIONI COMPLEMENTARI

L'Amministrazione rende noto che:

- Il finanziamento del servizio è effettuato con fondi regionali.
- **L'Amministrazione si riserva comunque la facoltà di non procedere ad alcuna aggiudicazione senza incorrere in responsabilità e/o azioni di risarcimento dei danni,** neanche ai sensi degli artt. 1337 e 1338 del codice civile anche qualora, in sede di aggiudicazione definitiva dell'appalto, non vi siano in bilancio le risorse necessarie.
- L'Amministrazione si riserva la facoltà insindacabile di non procedere all'indizione di un bando di gara, annullare o revocare il bando di gara, di prorogare la data di scadenza di presentazione delle offerte, dandone comunque comunicazione a concorrenti, senza ricorrere in alcuna responsabilità e senza che gli stessi possano fare richiesta di danni, indennità compensi o azioni di qualsiasi tipo.
- **L'Amministrazione si riserva la facoltà di non aggiudicare il servizio**, ai sensi del d.lgs. 50/2016 s.m.i. qualora ritenga, a suo insindacabile giudizio, che nessuna proposta risulti conveniente o idonea in relazione all'oggetto del contratto. In questo caso le imprese concorrenti non possono sollevare eccezioni.
- L'Amministrazione si riserva la facoltà di invitare, se necessario, i concorrenti a completare o a fornire chiarimenti in ordine al contenuto, dei certificati dei documenti e delle dichiarazioni presentati.
- La **proposta è immediatamente impegnativa per la Ditta** e lo sarà per l'Amministrazione solo successivamente all'adozione del provvedimento di aggiudicazione definitiva. L'aggiudicazione definitiva sarà comunque subordinata alla verifica del possesso in capo all'aggiudicatario dei requisiti di ordine generale e speciale nei modi e nei termini stabiliti dal d.lgs. 50/2016 s.m.i., nonché agli adempimenti connessi alla stipulazione del contratto. In ogni caso la presente lettera d'invito non è vincolante per l'Amministrazione, la quale, a proprio insindacabile giudizio, si riserva di non aggiudicare e di procedere ad un nuovo esperimento nei modi che riterrà più opportuni.
- Qualora venissero presentate dichiarazioni mendaci rese dai concorrenti ai sensi del D.P.R. 28.12.2000, n. 445, ovvero venissero formati atti falsi ai sensi del medesimo DPR 445/2000, l'Amministrazione trasmetterà la comunicazione di reato alla procura della Repubblica competente ai fini dell'applicazione delle sanzioni penali previste dall'art. 76 del medesimo decreto.
- Sono a totale carico della ditta aggiudicataria tutte le spese inerenti al contratto, oneri fiscali di bollo e di registro del contratto o di altro documento sostitutivo per l'affidamento, nonché ogni altro onere connesso al servizio o comunque discendente dall'applicazione del contratto stesso, senza diritto di rivalsa.
- In caso di fallimento della ditta aggiudicataria, l'affidamento s'intenderà senz'altro revocato e l'Amministrazione provvederà a termini di legge.

TITOLO IV
ADDENDUM PRIVACY

Il presente Allegato è redatto in conformità a quanto previsto all'art. 28 del Regolamento (UE) 2016/679 e forma parte integrante e sostanziale del Contratto stipulato tra le Parti.
Il Fornitore si impegna a presentare all'Amministrazione garanzie in termini di conoscenza specialistica, affidabilità, risorse, nonché in ordine all'adozione di misure tecniche, logiche ed organizzative adeguate per assicurare che i trattamenti dei dati personali siano conformi alle esigenze del Regolamento Europeo e, dunque, ai sensi dell'articolo 28 del Regolamento Europeo e con la sottoscrizione del contratto dichiara di essere consapevole, in ragione delle prestazioni da eseguire con lo specifico affidamento, di poter essere nominato in corso di esecuzione contrattuale con il verbale di affidamento come Responsabile esterno dei trattamenti di dati, in qualità di Responsabile primario.
Il mancato rispetto da parte del Responsabile primario o del sub-Responsabile del trattamento delle disposizioni di cui al presente Allegato sarà considerato un grave inadempimento del Contratto stesso.
Ai fini del presente Atto con il termine "Fornitore" si individua l'Impresa appaltatrice designata quale Responsabile primario, in funzione della designazione fatta dall'Amministrazione in qualità di Titolare in ragione delle prestazioni richieste in corso di esecuzione contrattuale.

29.Oggetto

Il presente Allegato disciplina le istruzioni che il Fornitore (ivi incluso il trattamento a opera di eventuale sub-appaltatore o sub-fornitore) si impegna ad osservare nell'ambito dei trattamenti dei dati personali che realizzerà per conto della Regione Piemonte quale Titolare (nel presente Allegato anche solo "**Amministrazione**") nello svolgimento delle attività oggetto del Contratto in essere con l'Amministrazione, garantendo il rispetto della normativa vigente in materia di tutela e sicurezza dei dati.

30.Definizioni

- "*Dati Personali dell'Amministrazione*": i Dati Personali (nonché i dati appartenenti alle categorie particolari di dati personali di cui all'art. 9 e 10 del Regolamento UE 2016/679), concessi in licenza o diversamente messi a disposizione, trasmessi, gestiti, controllati o comunque trattati dall'Amministrazione;
- "*Norme in materia di Trattamento dei Dati Personali*": tutte le leggi, disposizioni e direttive normative applicabili in relazione al trattamento e/o alla protezione dei Dati Personali, così come modificate di volta in volta, ivi incluso, ma non limitatamente, il Regolamento UE 2016/679 (GDPR), la normativa di adeguamento italiana, circolari, pareri e direttive dell'Autorità di Controllo nazionale, le decisioni interpretative adottate dallo *European Data Protection Board*.
- "*Contratto*": si intende il contratto stipulato tra l'Amministrazione e il Fornitore e avente ad oggetto Sviluppo piattaforma software Portale Antisofisticazioni vinicole della Regione Piemonte e strumenti correlati, monitoraggio e-commerce, analisi informatiche a sostegno dell'attività sei SAA, dei documenti reperiti sul *web, web marketing, web reputation*, analisi dei metadati, acquisizione informazioni da fonti aperte, assistenza e manutenzione portale, erogazione servizi specialistici legati alle attività di vigilanza e presidio del territorio e all'implementazione dei disposti di legge di cui all'art. 52 comma 2 lettera f) della l.r. n. 1/2019
- "*Misure di Sicurezza*": le misure di sicurezza di natura fisica, logica, tecnica e organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi comprese quelle specificate nel Contratto, unitamente ai suoi Allegati.

- "*Dati Personali*": qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) come definita nelle Norme in materia di Trattamento dei Dati Personali.
- "*Trattamento*": qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insieme di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o, qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione.
- "*Titolare del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione europea o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; ovvero l'Amministrazione.
- "*Responsabile del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare o del Contitolare del trattamento; ovvero il Fornitore;
- "*Sub-Responsabile del trattamento*": la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che svolge in forza di contratto scritto con altro Responsabile del trattamento; ovvero il subappaltatore o subfornitore autorizzato dall'Amministrazione;
- "*Fornitore*": l'Impresa appaltatrice designata quale Responsabile primario, in funzione della designazione fatta dall'Amministrazione in qualità di Titolare;
- "*Persone autorizzate al trattamento dei dati*": persone che in qualità di dipendenti, collaboratori, amministratori o consulenti del responsabile e/o del sub-responsabile siano state autorizzate al trattamento dei dati personali sotto l'autorità diretta del Responsabile primario o del Sub responsabile;
- "*Terzi autorizzati*": persone terze, ovvero la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento, che in qualità di dipendenti, collaboratori, amministratori (anche amministratori di sistema) o consulenti del Fornitore siano state autorizzate al trattamento dei dati personali sotto l'autorità diretta del Responsabile primario o del Sub- Responsabile;
- "*Violazione dei dati personali (data breach)*": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- "*Incidente di sicurezza*": la violazione di sicurezza che comporta la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati e/o informazioni riservate (non dati personali), la violazione e/o il malfunzionamento di misure di sicurezza, di strumenti elettronici, hardware o software a protezione dei dati e delle informazioni.

31.Sicurezza dei dati personali

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, nell'ambito delle proprie attività e competenze specifiche, un adeguato livello di sicurezza dei trattamenti, inclusa la riservatezza, 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.

32.Obblighi e istruzioni per il fornitore

32.1 Obblighi generali del fornitore

Il Fornitore è autorizzato a trattare per conto dell'Amministrazione i dati personali necessari per l'esecuzione delle attività di cui all'oggetto del Contratto.
A tal fine il Fornitore si impegna a:

- non determinare o favorire mediante azioni e/o omissioni, direttamente o indirettamente, la violazione da parte dell'Amministrazione delle Norme in materia di Trattamento dei Dati Personali;
- trattare i Dati Personali esclusivamente in conformità alle istruzioni documentate dell'Amministrazione, nella misura ragionevolmente necessaria all'esecuzione del Contratto, e alle Norme in materia di Trattamento dei Dati Personali;
- adottare, implementare e aggiornare Misure di sicurezza 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.

Il Fornitore si impegna a designare la figura professionale del Responsabile della protezione dei dati di cui all'art. 37 GDPR e a comunicarne i dati e i contatti di riferimento tempestivamente all'Amministrazione, in ragione dell'attività svolta.

33.Istruzioni per il Fornitore

33.1 Elementi essenziali dei trattamenti che il fornitore è stato autorizzato a svolgere dall'amministrazione

Gli elementi essenziali del trattamento sono contenuti nel presente documento, nel contratto e nei suoi allegati, nonché nei documenti tecnico – funzionali che saranno rilasciati dall'Amministrazione unitamente al verbale di affidamento in ragione delle prestazioni richieste in corso di esecuzione contrattuale.
In particolare i citati documenti conterranno, la materia disciplinata, la natura e finalità del trattamento, il tipo di dati personali trattati e le categorie di Interessati.
Salvo quanto dovesse essere previsto nei documenti di cui al presente paragrafo, le Parti si danno reciprocamente atto che, alla Data di Efficacia del presente Allegato:

- le attività che prevedono il trattamento dei dati dell'Amministrazione sono:
    - lo sviluppo delle applicazioni oggetto del Contratto che tratteranno i dati del Portale SAA;
    - il test e il collaudo del software applicativo oggetto del Contratto per effettuare i quali il Fornitore accede ai dati del Portale SAA previa adozione delle misure di sicurezza previste (anonimizzazione);

la durata del trattamento dei dati personali è limitata, dunque coincide, con la durata del Contratto e delle sue eventuali proroghe; limitatamente ai dati di test e di collaudo, la durata del trattamento è limitata alla durata del test e/o del collaudo e comunque termina con la fine del rapporto contrattuale e delle sue eventuali proroghe;
la natura e lo scopo del trattamento, tenuti conto i requisiti di legittimità stabiliti dalle leggi vigenti in materia di protezione dei dati, sono lo sviluppo e la manutenzione del software applicativo oggetto del Contratto;

i Dati Personali dell'Amministrazione sono i dati del sistema informativo del Portale SAA trattati dal Fornitore, per l'effettuazione di test e/o di collaudi applicativi, e sono "anonimizzati"; i dati connessi alla gestione del Contratto sono i dati personali relativi al personale che accede al portale SAA;
il Fornitore, al temine delle attività di test e/o collaudo delle applicazioni e comunque entro il termine della durata del Contratto, come eventualmente prorogato, elimina, con tecniche adeguate e sicure, i dati del sistema informatico del Portale SAA in suo possesso;

33.3 Obblighi del responsabile del trattamento nei confronti dell'amministrazione

Il Responsabile del trattamento si impegna a:

1. trattare i dati solo per l'esecuzione delle attività di cui all'oggetto del Contratto;
2. trattare i dati conformemente alle istruzioni documentate impartite dall'Amministrazione con il presente Allegato e con eventuali istruzioni documentate aggiuntive. Qualora il Fornitore reputi che un'istruzione sia, o possa essere, contraria alla Normativa in materia di protezione dei dati, ivi incluso il GDPR, deve informarne immediatamente l'Amministrazione;
3. trattare i dati conformemente alle istruzioni documentate dell'Amministrazione di cui al precedente comma anche nei casi di trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Fornitore; in tale ultimo caso il Fornitore dovrà informare l'Amministrazione di tale obbligo giuridico prima che il trattamento abbia inizio, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
4. garantire che il trattamento dei Dati Personali sia effettuato in modo lecito, corretto, adeguato, pertinente e avvenga nel rispetto dei principi di cui all'artt. 5 e ss. del GDPR.
5. garantire la riservatezza dei dati personali trattati per l'esecuzione delle attività del Contratto;
6. garantire che le persone autorizzate a trattare i dati personali in virtù del presente Contratto:
    - **i)** si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
    - **ii)** abbiano ricevuto, e ricevano, da parte del Fornitore la formazione necessaria in materia di protezione dei dati personali;
    - **iii)** accedano e trattino i dati personali osservando le istruzioni impartite dall'Amministrazione.
7. tenere conto nell'esecuzione delle attività contrattuali dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (*privacy by design e by default*) anche mediante l'ausilio delle istruzioni documentate impartite dal Titolare del trattamento;
8. conferire all'Amministrazione eventuale copia dei dati personali dei dipendenti, amministratori, consulenti, collaboratori o altro personale del Fornitore nel corso delle attività oggetto del Contratto esclusivamente per finalità relative all'esecuzione delle attività contrattuali ed amministrativo-contabili oltre che per la sicurezza delle sedi e dei sistemi. Il Fornitore, con la sottoscrizione dell'Addendum, autorizza l'Amministrazione, esclusivamente per le suddette finalità, ad estrarre tali dati personali dai propri sistemi informativi.

Qualora richiesto dalle Norme in materia di Trattamento dei Dati Personali, l'Amministrazione e il Fornitore convengono di sottoscrivere un accordo aggiuntivo, di modifica o di aggiornamento che potrà essere necessario anche per consentire il trasferimento di tali dati personali qualora non rientrino nella sua giurisdizione di origine ai sensi delle Norme sul Trattamento dei Dati Personali.

33.4 Obblighi del fornitore nell'ambito dei diritti esercitati dagli interessati nei confronti dell'amministrazione.

Il Fornitore deve collaborare e supportare nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del GDPR, ovverosia alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.
Il Fornitore deve dare supporto, in tale attività, affinché il riscontro alle richieste di esercizio dei diritti degli Interessati avvenga senza giustificato ritardo.
A tal fine il Fornitore deve adottare e aggiornare un registro di tutte le attività di trattamento eseguite per conto dell'Amministrazione completo di tutte le informazioni previste all'art. 30 del GDPR (cfr. successivo paragrafo III del presente Allegato) e mettere tale registro a disposizione dell'Amministrazione affinché si possa ottemperare senza ingiustificati ritardi alle istanze formulate dagli Interessati ai sensi degli artt. 15-23 del GDPR.
Qualora gli Interessati esercitino un diritto previsto dal GDPR trasmettendo la relativa richiesta al Fornitore, quest'ultimo deve inoltrarla tempestivamente, e comunque entro e non oltre 3 giorni dalla ricezione, per posta elettronica all'Amministrazione.

33.5 Obblighi del fornitore che ricorre a terzi autorizzati

Il Fornitore può ricorrere a Terzi Autorizzati per l'esecuzione di specifiche attività di trattamento esclusivamente nei casi in cui abbia ricevuto espressa autorizzazione scritta dall'Amministrazione.
Nell'ipotesi in cui il Fornitore, previa autorizzazione scritta dell'Amministrazione, abbia designato un Terzo Autorizzato, il Fornitore e il Terzo autorizzato dovranno essere vincolati da un accordo scritto recante tutti gli obblighi in materia di protezione dei dati di cui al presente Contratto e relativi Allegati e di cui alle ulteriori eventuali istruzioni documentate aggiuntive impartite dall'Amministrazione.
Il Fornitore deve formulare per iscritto all'Amministrazione la domanda di autorizzazione alla nomina di un Terzo Autorizzato, specificando:

a. i) le attività di trattamento da delegare;
b. il nominativo/ragione sociale e gli indirizzi del Terzo;
c. i requisiti di affidabilità ed esperienza - anche in termini di competenze professionali, tecniche e organizzative nonché con riferimento alle misure di sicurezza - del Terzo in materia di trattamento dei dati personali;
d. il contenuto del relativo contratto tra il Fornitore e il Terzo autorizzato.

In particolare, il Fornitore deve garantire che il Terzo Autorizzato assicuri l'adozione di misure, logiche, tecniche ed organizzative adeguate di cui al presente contratto ed alla normativa e regolamentazione in materia ed alle istruzioni impartite dall'Amministrazione in materia di protezione dei dati personali.
Resta, in ogni caso, ferma la successiva facoltà dell'Amministrazione di opporsi all'aggiunta o sostituzione del Terzo Autorizzato con altri soggetti Terzi.
Le istruzioni impartite dal Fornitore a qualsiasi Terzo dovranno avere il medesimo contenuto e perseguire i medesimi obiettivi delle istruzioni fornite al Fornitore dall'Amministrazione nei limiti dei trattamenti autorizzati in capo al Terzo.
A tal fine, l'Amministrazione può in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del Terzo Autorizzato, anche per mezzo di *audit*, *assessment*, sopralluoghi e ispezioni svolti mediante il proprio personale oppure tramite soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti l'Amministrazione, in conformità a quanto contrattualmente previsto, può risolvere il contratto con il Fornitore. Nel caso in cui all'esito delle verifiche, ispezioni,

audit e assessment le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione delle Norme in materia di protezione dei dati personali, l'Amministrazione applicherà al Fornitore una penale come contrattualmente previsto e diffiderà lo stesso a far adottare al Terzo Autorizzato tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato (tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia dei dati e della categoria dei soggetti interessati coinvolti nonché del livello di rischio relativo alla violazione dei dati, alla gravità della violazione verificatasi e degli incidenti di sicurezza). In caso di mancato adeguamento da parte del Terzo Autorizzato e/o del Fornitore a tale diffida l'Amministrazione potrà risolvere il Contratto ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.

33.6 Il registro dei trattamenti del fornitore

Il Fornitore è obbligato a predisporre, conservare, aggiornare - anche con l'ausilio del proprio Responsabile della protezione dei dati - un registro, in formato elettronico di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Titolare del Trattamento, come prevede l'art. 30, comma 2, del GDPR.
In particolare, il Registro del Fornitore dei trattamenti svolti per conto dell'Amministrazione deve contenere:

a. il nome e i dati di contatto del Fornitore (e, se del caso, di Terzi Autorizzati) del trattamento, di ogni Titolare del trattamento per conto del quale il Fornitore agisce, del rappresentante (eventuale) del Fornitore e del Terzo Autorizzato, nonché del Responsabile della protezione dei dati (DPO);
b. le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
c. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate;
d. una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto per un trattamento corretto e sicuro ai sensi dell'articolo 32 del GDPR

33.7 Obblighi di supporto, collaborazione e coordinamento del responsabile del trattamento nell'attuazione degli obblighi dell'amministrazione

Il Responsabile del trattamento assiste e collabora pienamente con l'Amministrazione nel garantire il rispetto degli obblighi di cui agli articoli 31, 32, 33, 34, 35 e 36 del GDPR, come di seguito descritto.

a) Misure di sicurezza.

Il Fornitore deve mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e garantire il rispetto degli obblighi di cui all'art. 32 del GDPR. I criteri per la valutazione del rischio devono essere previamente condivisi e approvati dall'Amministrazione. 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.

Il Fornitore si obbliga ad adottare le misure di sicurezza previste da codici di condotta di settore ove esistenti e dalle certificazioni ove acquisite (art. 40 - 43 GDPR)].
Nel valutare l'adeguatezza del livello di sicurezza il Fornitore deve tenere 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, o dal trattamento non consentito o non conforme alle finalità della raccolta, ai dati personali trasmessi, conservati o comunque trattati.
Nell'effettuare l'analisi dei rischi il Fornitore utilizza i criteri di valutazione del rischio condivisi ed approvati dall'Amministrazione. All'esito dell'analisi dei rischi, le misure di sicurezza adeguate ai sensi dell'art. 32 del GDPR devono essere condivise ed approvate dall'Amministrazione.
I risultati dell'analisi del rischi per l'individuazione delle misure di sicurezza adeguate andranno riportati dal Fornitore in un apposito documento contenente almeno le seguenti informazioni: identificazione e classificazione dei dati personali trattati anche in termini di riservatezza ed integrità; classificazione del trattamento anche in termini di disponibilità; valutazione dei rischi per l'interessato e inerenti il trattamento stesso; l'identificazione delle misure di sicurezza così come richieste ai sensi dell'articolo 32 del GDPR.
L'attività di identificazione dei dati personali oggetto del trattamento dovrà seguire i criteri di privacy by default di cui all'art. 25 del GDPR
Ai sensi dell'art. 32, comma 4, GDPR il Fornitore deve garantire che chiunque agisca sotto la sua autorità e abbia accesso ai Dati Personali non tratti tali dati se non debitamente istruito, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

a) Obblighi del Fornitore nelle ipotesi di "data breach"

Il Fornitore deve assistere e collaborare pienamente con l'Amministrazione, nelle attività di adempimento di cui agli articoli 33 e 34 del GDPR in materia di violazioni di dati personali, ovvero di *data breach*.
In particolare, il Fornitore deve:

a. predisporre e aggiornare un registro contenente tutte le violazioni dei dati personali sia dai trattamenti eseguiti per conto dell'Amministrazione, al fine di facilitare quest'ultima nelle attività di indagine a seguito di *data breach*;
b. comunicare all'Amministrazione, tempestivamente e in ogni caso senza ingiustificato ritardo, che si è verificata una violazione dei dati personali da quando il Fornitore, o un suo Terzo Autorizzato, ne ha avuto conoscenza o ha avuto elementi per sospettarne la sussistenza. Tale comunicazione deve essere redatta in forma scritta, in modo conforme ai criteri previsti dall'art. 33 del GDPR e deve essere trasmessa unitamente a ogni documentazione utile all'Amministrazione per consentirle di notificare la violazione all'Autorità di controllo competente entro e non oltre il termine di 72 ore da quando ne ha avuto conoscenza;
c. indagare sulla violazione di dati personali adottando tutte le misure tecniche e organizzative e le misure rimediali necessarie a eliminare o contenere l'esposizione al rischio, collaborare con l'Amministrazione nelle attività di indagine, mitigando qualsivoglia danno o conseguenza lesiva dei diritti e delle libertà degli Interessati (misure di mitigazione) nonché ponendo in atto un piano di misure, previa approvazione dell'Amministrazione, per la riduzione tempestiva delle probabilità che una violazione simile di dati personali possa ripetersi;
d. nel caso in cui l'Amministrazione debba fornire informazioni (inclusi i dettagli relativi ai servizi prestati dal Fornitore) all'Autorità di controllo il Fornitore supporterà l'Amministrazione nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Fornitore e/o di suoi Terzi Autorizzati

34. Obblighi del fornitore nella valutazione d'impatto del rischio di violazioni dei dati personali.

Per svolgere la valutazione d'impatto dei trattamenti sulla protezione dei dati personali l'Amministrazione può consultarsi con il proprio Responsabile della protezione dei dati (art. 35, comma 2, del GDPR).
Il Responsabile del trattamento si impegna ad assistere l'Amministrazione, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come disciplinata dall'art. 35 del GDPR, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali (di seguito anche "**PIA**") o dell'aggiornamento della PIA.
I risultati della valutazione d'impatto ex art. 35 del GDPR per l'individuazione delle misure di sicurezza necessarie andranno riportati dal Fornitore nel documento di analisi del rischio di cui al precedente art. 33).
Il Fornitore si impegna altresì ad assistere l'Amministrazione nell'attività di consultazione preventiva dell'Autorità di controllo ai sensi dell'articolo 36 del GDPR.

35. Ulteriori obblighi di garanzia del fornitore del trattamento.

Il Fornitore si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali siano precisi, corretti e aggiornati durante l'intera durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Fornitore, o da un Terzo da lui autorizzato, nella misura in cui il Fornitore sia in grado di operare in tal senso.
Il Fornitore si impegna a trasmettere all'Amministrazione tutte le informazioni e la documentazione che quest'ultima potrà ragionevolmente richiedere durante il Contratto al fine di verificare la conformità del Fornitore (o del Terzo Autorizzato come sub-appaltatore e sub-fornitore) con il presente Allegato, le Norme in materia di Trattamento dei Dati Personali e le Misure di sicurezza.
Il Fornitore garantisce all'Amministrazione, o ai suoi rappresentanti debitamente autorizzati, la possibilità di svolgere, con ragionevole preavviso, attività di controllo e valutazione, anche mediante ispezioni e sopralluoghi condotte da soggetti autorizzati e incaricati dall'Amministrazione, delle attività di trattamento dei Dati Personali eseguite dal medesimo Fornitore, ivi incluso l'operato degli eventuali amministratori di sistema, allo scopo di verificarne la conformità con il Contratto (ivi inclusi i rispettivi Allegati), con le Istruzioni dell'Amministrazione e le Norme in materia di Trattamento dei Dati. Il Fornitore deve mettere a disposizione dell'Amministrazione senza alcun ritardo e/o omissione, tutte le informazioni necessarie per dimostrare la sua conformità con gli obblighi previsti nel Contratto. Nel caso in cui all'esito delle verifiche periodiche, delle ispezioni, *audit* e *assessment* le misure tecniche, organizzative e/o di sicurezza risultino inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, l'Amministrazione applicherà al Fornitore le penali previste dal Contratto diffidandolo ad adottare le misure necessarie entro un termine congruo che sarà all'occorrenza fissato (tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia dei dati e della categoria dei soggetti interessati coinvolti nonché del livello di rischio violazione e/o della gravità della violazione verificatasi). In caso di mancato adeguamento da parte del Fornitore a tale diffida l'Amministrazione potrà risolvere il Contratto ed escutere la garanzia definitiva, fatto salvo il risarcimento del maggior danno.
Fatto salvo quanto previsto al successivo paragrafo VI il Fornitore non può trasferire i Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto autorizzazione scritta da parte dell'Amministrazione.

Il Fornitore si impegna a notificare tempestivamente all'Amministrazione ogni provvedimento di un'Autorità di controllo, o dell'Autorità giudiziaria relativo ai Dati Personali dell'Amministrazione salvo il caso in cui tale comunicazione non sia vietata dal provvedimento o dalla legge.
In simili circostanze, salvo divieti previsti dalla legge, il Fornitore deve: i) informare l'Amministrazione tempestivamente, e comunque entro 24 ore dal ricevimento della richiesta di ostensione; ii) collaborare con l'Amministrazione, nell'eventualità in cui lo stesso intenda opporsi legalmente a tale comunicazione; iii) garantire il trattamento riservato di tali informazioni.
Il Fornitore prende atto e riconosce che, nell'eventualità di una violazione delle disposizioni del presente Allegato, oltre all'applicazione delle clausole di risoluzione del contratto e delle penali, nonché all'eventuale risarcimento del maggior danno, l'Amministrazione 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 manleverà e terrà indenne l'Amministrazione da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione delle Norme in materia di Trattamento Personali e/o del Contratto (inclusi gli Allegati) comunque derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o Terzi autorizzati (sub-fornitori).

36. Trasferimenti dei dati personali verso paesi terzi o organizzazioni internazionali

L'Amministrazione può autorizzare per iscritto il Fornitore, o un suo Terzo Autorizzato, al trasferimento dei Dati personali (o parte di tali dati) verso paesi terzi o organizzazioni internazionali nelle sole ipotesi in cui il paese terzo o l'organizzazione internazionale sia stata oggetto di una valutazione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, oppure, in alternativa, previo rilascio della valutazione di adeguatezza svolta dal Titolare ai sensi dell'art. 46 del GDPR.
Nel caso in cui l'Amministrazione, in relazione all'esecuzione da parte del Fornitore del trattamento dei suoi servizi e/o all'adempimento degli obblighi assunti con il Contratto, consenta al Fornitore (o a un sub-fornitore) il trasferimento dei dati Personali verso paesi terzi o organizzazioni internazionali, il Fornitore deve: - convenire (e impegnarsi affinché i suoi sub-fornitori convengano) di ottemperare agli obblighi previsti nelle clausole del Contratto;
garantire che, prima di tale trasferimento, l'Amministrazione e/o il Fornitore stipulino un accordo per l'accesso ai dati come indicato dalla Commissione Europea; inserire nell'accordo di trasferimento dei Dati personali le disposizioni delle clausole contrattuali e delle Norme applicabili in materia di Trattamento dei Dati Personali.

37. Obblighi del fornitore del trattamento al termine del contratto.

Il Fornitore si impegna a non conservare - nonché a garantire che i Terzi autorizzati non conservino - i Dati Personali per un periodo di tempo ulteriore al limite di durata strettamente necessario per l'esecuzione dei servizi e/o l'adempimento degli obblighi di cui al Contratto, o così come richiesto o permesso dalla legge applicabile.
Alla scadenza del Contratto o al termine della fornitura dei servizi relativi al Trattamento dei Dati il Fornitore dovrà cancellare o restituire in modo sicuro all'Amministrazione tutti i Dati Personali nonché cancellare tutte le relative copie esistenti, fatto salvo quanto diversamente disposto dalle Norme in materia di Trattamento dei Dati Personali. Il Fornitore deve documentare per iscritto all'Amministrazione tale cancellazione.

38. Modifiche delle leggi in materia di trattamento dei dati personali

Nell'eventualità di qualsivoglia modifica delle Norme in materia di Trattamento dei Dati Personali applicabili al trattamento dei Dati Personali, che generi nuovi requisiti (ivi incluse nuove misure di natura fisica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Fornitore collaborerà con l'Amministrazione, nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti durante l'esecuzione del Contratto.

TITOLO V
INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ARTICOLO 13 GDPR 679/2016

I dati personali richiesti dalla stazione appaltante alle ditte concorrenti sono raccolti e trattati nel rispetto dei principi di correttezza, liceità e tutela della riservatezza, con modalità informatiche ed esclusivamente per finalità di trattamento dei dati personali espressi nella presente dichiarazione e comunicati a **Regione Piemonte, Settore A1706A Servizi di sviluppo e controlli in agricoltura**. I dati acquisiti a seguito della presente informativa sono utilizzati esclusivamente per le finalità per le finalità inerenti al presente esperimento di mercato;

il trattamento dei dati avverrà mediante strumenti, anche informatici, idonei a garantirne la sicurezza e la riservatezza, limitatamente e per il tempo necessario agli adempimenti relativi alla procedura di cui all'oggetto;

il conferimento dei dati ha natura obbligatoria, poiché un eventuale rifiuto a rendere le dichiarazioni e le documentazioni, richieste dalla stazione appaltante in base alla vigente normativa, comporterà l'esclusione dall'esperimento di mercato;

i dati e i documenti saranno rilasciati agli organi dell'autorità giudiziaria che ne facciano richiesta, nell'ambito del procedimento a carico delle ditte concorrenti;

i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati sono:

a. il personale interno dell'Amministrazione che cura il procedimento amministrativo o, comunque, in esso coinvolto per ragioni di servizio;
b. ogni altro soggetto che abbia interesse ai sensi della legge 241/90 s.m.i, della legge regionale 7/2005 e del d.lgs. 50/2016 s.m.i;
c. ai soggetti destinatari delle comunicazioni e della pubblicità previste dalla legge e dai regolamenti approvati in materia di appalti;

i dati di contatto del Responsabile della protezione dati (DPO) sono: dpo@regione.piemonte.it, Piazza Castello 165, 10121 Torino;

il Titolare del trattamento dei dati personali è la Giunta regionale, il delegato al trattamento dei dati è il Dirigente regionale della Direzione Agricoltura competente in materia di Servizi di sviluppo e controlli in agricoltura, C.so Stati Uniti, 21 Torino;

i Responsabili (esterni) del trattamento sono: CSI Piemonte, con sede in Torino, Corso Unione Sovietica 216 nella persona del suo Legale Rappresentante, i cui dati di contatto sono: protocollo@cert.csi.it e privacy@csi.it;

i dati sono trattati esclusivamente da soggetti incaricati e Responsabili (esterni) individuati dal Titolare, o da soggetti incaricati individuati dal Responsabile (esterno), autorizzati ed istruiti in tal senso, adottando tutte quelle misure tecniche ed organizzative adeguate a tutelare i diritti, le libertà e i legittimi interessi che Le sono riconosciuti per legge in qualità di Interessato;

i dati personali non sono in alcun modo oggetto di trasferimento in un Paese terzo extraeuropeo, né di comunicazione a terzi fuori dai casi previsti dalla normativa in vigore, né di processi decisionali automatizzati compresa la profilazione;

è possibile esercitare i diritti previsti dagli artt. da 15 a 22 del regolamento UE 679/2016, quali: la conferma dell'esistenza o meno dei suoi dati personali e la loro messa a disposizione in forma intellegibile; avere la conoscenza delle finalità su cui si basa il trattamento; ottenere la cancellazione,

la trasformazione in forma anonima, la limitazione o il blocco dei dati trattati in violazione di legge, nonché l'aggiornamento, la rettifica o, se vi è interesse, l'integrazione dei dati; opporsi, per motivi legittimi, al trattamento stesso, rivolgendosi al Titolare, al Responsabile della protezione dati (DPO), o al Responsabile del trattamento tramite i contatti di cui sopra o il diritto di proporre reclamo all'Autorità di controllo competente (Garante per la protezione dei dati personali: garante@gpdp.it).

Responsabile del procedimento: Elena Russo – A1706A Servizi di sviluppo e controlli in agricoltura – Corso Stati Uniti 21 – 10128 Torino – Tel. 011.432.14.66 | Fax. 011.437.72