CITTÀ METROPOLITANA DI PALERMO

DIREZIONE GARE E CONTRATTI – INNOVAZIONE TECNOLOGICA

UFFICIO INNOVAZIONE DIGITALE

SERVIZI OPERATIVI A SUPPORTO PER IL CONSOLIDAMENTO ED EVOLUZIONE DEL PRODOTTO EDR OPEN-SOURCE WAZUH ATTUALMENTE IN USO PRESSO L'AMMINISTRAZIONE

☒ CAPITOLATO SPECIALE D'ONERI

Il Responsabile del Procedimento

Dott. F. Brugè

Firmato digitalmente da:
Filippo Brugè
Data: 16/06/2025 15:50:11

CAPITOLATO SPECIALE D'ONERI

SERVIZI OPERATIVI A SUPPORTO PER IL CONSOLIDAMENTO ED EVOLUZIONE DEL PRODOTTO EDR OPEN-SOURCE WAZUH ATTUALMENTE IN USO PRESSO L'AMMINISTRAZIONE

Art. 0
(Premessa)

Il presente Capitolato disciplina la fornitura, per la Città Metropolitana di Palermo, dei servizi operativi a supporto per il consolidamento ed evoluzione del prodotto EDR open-source Wazuh attualmente in uso presso l'amministrazione, specificando le condizioni e le modalità di erogazione dei Servizi connessi alla fornitura.

Nel corpo del Capitolato e nei suoi allegati, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- **Capitolato:** il presente documento
- **Fornitura:** i servizi operativi a supporto per il consolidamento ed evoluzione del prodotto EDR open-source Wazuh attualmente in uso presso l'amministrazione
- **Ditta:** la ArcaSafe S.r.l.
- **Fornitore:** la ArcaSafe S.r.l.
- **Amministrazione:** la Città Metropolitana di Palermo

Art. 1
(Oggetto dell'Appalto)

Il presente capitolato ha per oggetto l'attività di erogazione dei servizi operativi a supporto per il consolidamento ed evoluzione del prodotto EDR open-source Wazuh attualmente in uso presso l'amministrazione.

Art. 2
(Servizi oggetto della fornitura)

- Fase 1: Fornitura istanza Wazuh on Cloud in SaaS
- Fase 2: Aggiornamento Istanza Wazuh on Premise presso il Datacenter dell'Amministrazione
- Fase 3: Incident response
- Fase 4: Servizi di Gestione, Amministrazione, assistenza
- Fase 5: Formazione

Descrizione delle attività previste nelle 5 fasi.

Fase 1: Fornitura istanza Wazuh on Cloud in SaaS

- Setup e Attivazione Piattaforma Wazuh on Cloud con le seguenti caratteristiche
  - Numero totale di Active Agents: 100 (Server e Apparati di rete)

    - Average/Peak EPS 100-500
    - Indexed Data Retention (giorni) 90
    - Archive Data Retention (mesi) 12
    - Maintenance & Upgrades to the latest version
- Attività di onBoarding che comprendono
    - allestimento di un di un syslog collector on Premise persso il datacenter della Amministrazione
    - configurazione dei server ed apparati di rete
    - collegamento alla istanza Wazuh on Cloud

.

Le attività a supporto della struttura IT dell'Amministrazione nel contesto degli obbiettivi di Fase 1, sono stimate in 12 mezze giornate.

FASE 2: Aggiornamento istanza Wazuh on Premise presso il Datacenter dell'Amministrazione

Sono previsti i seguenti interventi finalizzati alla gestione ottimizzata dell'istanza on premise presso il Datacenter dell'Amministrazione:

- Aggiornamento e installazione SW Wazuh on Premise
- Integrazione con istanza Wazuh onCloud – (Server e Apparati di rete)
- Test e messa in opera

Le attività a supporto della struttura IT dell'Amministrazione nel contesto degli obbiettivi di Fase 2, sono stimate in 13 mezze giornate

FASE 3: Incident response

Per un periodo di dodici mesi dalla data del collaudo sarà disponibile :

- Servizio Pronto Intervento – disponibile 24 x 7 (per 1 intervento) che comprende:
    - Configurazione Jump-box per analisi evento
    - Isolamento dispositivi attaccati – ove possibile

- Piattaforma Exigence on Cloud per la gestione della Procedura di Incident Response che comprende:
    - Supporto tecnico e legale per lo sviluppo della procedura
    - Implementazione attività di intervento
    - Gestione attività di intervento e produzione report
    - Formazione personale tecnico per Implementazione

- Valutazione d'Impatto DPIA – ex art. 35/GDPR –
    - per trattamento controllo attività lavoratori

Le attività a supporto della struttura IT dell'Amministrazione nel contesto degli obbiettivi di Fase 3, sono quantificate in 15 mezze giornate.

FASE 4: Servizi di Gestione, Amministrazione, assistenza

I servizi di Gestione, Amministrazione, assistenza comprendono:

- Report Risk Assessment – inizio Attività 1
- Report Risk Assessment – fine anno 1
- Support Coverage 8h x 5 dd
- Maximum response time 8 business hours

- Technical inquiries Unlimited
- Assisted upgrades to the newest version
- Audit Report – System's Health Checks n.ro 2 Report
- SOC Monitoring & Warning SLA 8/5
- MSP Support - SOC Control Room 12 mesi
- DTI – Domain Threat Intelligence n.ro 6 Report :
- Analisi Risorse 2° e 3° livello pubblicate in Internet
- e-MTI – eMail Threat Intelligence
  Discovery credenziali compromesse in Deep/Dark Web

Le attività a supporto della struttura IT dell'Amministrazione nel contesto degli obbiettivi di Fase 3, sono quantificate in 18 mezze giornate.

FASE 5: Formazione

I servizi di formazione verranno erogati con le seguenti modalità:
- Training on the job
- Numero 3 partecipanti

Le attività di formazione a supporto della struttura IT dell'Amministrazione nel contesto degli obbiettivi di Fase 5, sono quantificate in 10 mezze giornate.

Art. 3

(Tempi della fornitura)

La Ditta si impegna a completare i servizi di cui all'Art. 2 entro 90 giorni naturali e consecutivi dalla stipula del Contratto.

Art. 4

(Garanzia)

Per il periodo di un anno dalla data del collaudo la Ditta garantisce il buon funzionamento dei servizi attivati, assumendo l'obbligo di porre rimedio alle problematiche che si dovessero evidenziare, senza alcun addebito.
L'Amministrazione è obbligata a informare prontamente la Ditta degli inconvenienti che si verificano, specificandone le caratteristiche.
La Ditta interviene e ripristina la piena funzionalità dei servizi entro il secondo giorno lavorativo successivo alla richiesta dell'Amministrazione. E' fatta salva l'applicazione delle penali di cui all'art. 6.
Qualora la Ditta provi che i guasti ed i malfunzionamenti siano stati determinati da colpa o dolo del personale appartenente all'Amministrazione o da questa incaricato, le spese della riparazione, che la Ditta è tenuta comunque ad eseguire nel termine di cui al comma 4, sono a carico dell'Amministrazione.

Art. 5

(Obblighi e responsabilità della Ditta)

La Ditta appaltatrice della fornitura disciplinata dal presente capitolato speciale d'Oneri è obbligata:
a. a porre in essere, con tempestività, ogni adempimento prescritto dall'Amministrazione e, conseguentemente alla rilevazione di difetti o imperfezioni o difformità nei software;
b. ad assumere in proprio ogni responsabilità in caso di infortuni o di danni arrecati eventualmente a persone o cose tanto dell'amministrazione che di terzi, a causa di

manchevolezze o trascuratezze nell'esecuzione delle prestazioni oggetto del presente capitolato;

c. ad ottemperare a tutti gli obblighi verso i propri dipendenti in conformità a quanto previsto dalle disposizioni legislative e regolamentari vigenti in materia di lavoro e di assicurazioni sociali assumendo a suo carico tutti gli oneri relativi; ad attuare nei confronti dei propri dipendenti impegnati nella prestazione disciplinata dal presente capitolato, condizioni normative e retributive non inferiori a quelle risultanti dai contratti collettivi di lavoro vigenti nelle località in cui viene svolta la prestazione. I suddetti obblighi vincolano la Ditta anche se non sia aderente alle associazioni stipulanti o receda da esse.

L'Amministrazione, in caso di violazione degli obblighi di cui sopra e previa comunicazione alla Ditta delle inadempienze ad essa denunciate dall'Ispettorato del lavoro, si riserva il diritto di operare una ritenuta pari, nel massimo, al 10% dell'importo contrattuale.

Art. 6

(Penali)

Qualora siano riscontrati dall'Amministrazione ritardi o inadempimenti da parte della Ditta nell'esecuzione delle prestazioni oggetto dell'affidamento, rispetto ai termini e alle modalità pattuite, quest'ultima contesterà formalmente alla Ditta l'inadempimento/ritardo rilevato, concedendogli un termine di cinque giorni lavorativi per poter produrre eventuali controdeduzioni. Trascorso inutilmente il predetto termine, ovvero qualora le giustificazioni addotte non siano riconosciute in tutto o in parte valide, l'Amministrazione provvederà all'applicazione della penale che complessivamente non potrà superare il 10% del valore dell'appalto.

Qualora si verifichi un ritardo rispetto ai tempi della fornitura di cui all'art. 3 per cause non imputabili all'Amministrazione, ovvero a forza maggiore o a caso fortuito, è applicata una penale pari all'1,5 per mille dell'ammontare netto contrattuale al giorno per ogni giorno solare di ritardo.
Qualora, a seguito della richiesta di assistenza di cui all'art. 4, non vengano rispettati i livelli servizio indicati, è applicata una penale pari all'1,5 per mille dell'ammontare netto contrattuale al giorno per ogni giorno solare di ritardo.
E' fatto salvo il risarcimento dell'eventuale maggior danno.

In caso di mancato rispetto delle regole di compliance dei "Principi e obblighi derivanti dal DNSH" si applica una penale pari al 1 (uno) per mille dell'ammontare netto contrattuale. Il mancato rispetto delle condizioni per la compliance al principio DNSH, attestato a seguito dei monitoraggi e delle verifiche svolte o richieste dall'Amministrazione, oltre all'applicazione delle penali nella misura stabilita nel contratto, costituisce causa di risoluzione di diritto dello stesso Contratto ai sensi dell'articolo 1456 del Codice Civile.

Nel caso in cui la Ditta abbia un numero di dipendenti compreso tra 15 e 50, in caso di ritardata consegna della relazione di genere sulla situazione del personale maschile e femminile rispetto al termine dei sei mesi dalla conclusione del contratto si applica una penale giornaliera per ogni giorno di ritardata consegna pari all' 1 per mille dell'ammontare netto contrattuale, fino al limite massimo del 10% dell'ammontare netto contrattuale così come stabilito dall'art. 50 del decreto legge 77/2021. La mancata produzione della suddetta relazione, fatta salva l'applicazione delle penali di cui al precedente periodo, determina inoltre per la Ditta l'interdizione alla partecipazione, per un periodo di dodici mesi, sia in forma singola sia in raggruppamento, ad ulteriori procedure di affidamento in ambito PNRR e PNC.

4. Nel caso in cui la Ditta abbia un numero di dipendenti superiore a 15, in caso di ritardata consegna della dichiarazione relativa all'assolvimento delle norme che disciplinano il diritto al lavoro delle persone con disabilità e della relazione relativa a tale assolvimento e alle eventuali sanzioni e provvedimenti nel triennio antecedente la data di scadenza di presentazione delle offerte, rispetto al termine dei sei mesi dalla conclusione del contratto ai sensi del precedente articolo (Responsabilità dell'affidatario e obblighi specifici derivanti dal PNRR), si applica una penale giornaliera per ogni giorno di ritardata consegna pari all'1 per mille dell'ammontare netto contrattuale, fino al limite massimo del 10% dell'ammontare netto contrattuale così come stabilito dall'art. 50 del decreto legge 77/2021.

Art. 7

(Risoluzione del contratto)

Nei casi di inadempienze della Ditta le quali si protraggono oltre il termine, non inferiore a quindici giorni, assegnato dall'Amministrazione per porre fine all'inadempimento, l'Amministrazione ha la facoltà di dichiarare risolto il contratto, nonché di procedere all'esecuzione in danno. Restano fermi l'applicazione delle penali ed il risarcimento dell'eventuale maggior danno.

Nel caso in cui la verifica a campione sulle dichiarazioni relative ai requisiti di ordine generale e di capacità tecnico professionale, ai sensi dell'art. 52, comma 1, del D.Lgs. n. 36/2023, sia negativa, si dà luogo alla risoluzione del contratto, se ancora in corso, ed al pagamento del corrispettivo solo con riferimento alle prestazioni già eseguite e nei limiti dell'utilità ricevuta. Si dà luogo, inoltre, alla comunicazione all'ANAC, alla sospensione della Deitta dalla partecipazione alle procedure di affidamento indette dall'Amministrazione per un periodo da uno a dodici mesi decorrenti dall'adozione del decreto che accerta l'esito negativo dei controlli e all'incameramento della garanzia definitiva, ove richiesta. In caso di risoluzione del contratto, l'Amministrazione procederà alla richiesta di risarcimento dei danni, anche derivanti dalla necessità di procedere ad un nuovo affidamento.
L'Amministrazione procederà alla risoluzione del contratto ai sensi dell'art. 1456 del codice civile anche nei seguenti casi:

- per quanto previsto all'art. 122, commi 1 e 2, del D.Lgs. n. 36/2023;
- in caso di transazioni finanziarie relative a tutte le attività di cui al presente contratto non effettuate in ottemperanza agli obblighi previsti dalla Legge n. 136 del 13.08.2010;
- in caso di subappalto non autorizzato dall'Amministrazione;
- in caso di cessione di tutto o parte del contratto.

Art. 8

(Modalità di pagamento)

La fattura elettronica intestata a Città Metropolitana di Palermo, codice fiscale 80021470820, Codice Univoco 4UV278 deve essere inviata tramite i canali e con le specifiche previste dal D.M. n. 55 del 03/04/2013 "Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica", con l'indicazione del codice CIG e del codice CUP e l'indicazione della Misura PNRR che finanzia il contratto. Per effetto della L. 190/2014, coordinata con il D.L. 50/2017 che dispone l'applicazione del regime dello "Split payment", il tracciato della fattura elettronica deve riportare nel campo "Esigibilità IVA" la lettera "S" (Scissione pagamenti).
La fattura dovrà essere unica e riferita all'intero corrispettivo contrattuale secondo il prezzo offerto dalla Ditta e dovrà essere emessa dopo che i prodotti sono stati sottoposti, con esito

positivo, alla verifica di regolare esecuzione nel termine massimo di due giorni lavorativi dalla comunicazione del rilascio del Certificato di regolare esecuzione con esito positivo da parte dell'Amministrazione. Il pagamento del corrispettivo viene effettuato **entro gg. 30** dalla presentazione della fattura.
La fattura deve essere in regola con le norme fiscali.

Art. 9

(Verifiche di regolare esecuzione)

La fornitura di cui al presente capitolato sarà sottoposta alla verifica di regolare esecuzione da parte del Responsabile Unico del Progetto (RUP) o del Direttore dell'Esecuzione (ove nominato) intesa a verificare, per i servizi oggetto della fornitura, che siano in grado di svolgere le funzioni richieste in ambiente di produzione.
Gli interventi di ordine tecnico degli incaricati delle verifiche e controllo non esimono, comunque, la Ditta da responsabilità per difetti o per qualunque difformità nelle caratteristiche della configurazione dei servizi che dovessero rilevarsi.
La verifica è effettuata non oltre trenta giorni dalla comunicazione della data di consegna.
Il Responsabile Unico del Progetto (RUP) così come previsto dall'art. 50, comma 7, del D.Lgs. n. 36/2023 e dall'art. 38 dell'Allegato II.14 del D.Lgs. n. 36/2023, emette quindi il Certificato di regolare esecuzione a seguito dei necessari accertamenti e ne rilascia copia conforme alla Ditta in modalità telematica.

Art. 10

(Controversie)

Per quanto non espressamente previsto si rimanda al regolamento di cui al DPCM 6/8/97 n. 452 approvativo del capitolato di cui all'art. 12 comma 1 del decreto legislativo 12/2/93 n. 39.
Qualsiasi controversia che dovesse insorgere in ordine al contratto tra l'Amministrazione appaltante e la Ditta ove l'Amministrazione sia attore o convenuto sarà di competenza della Autorità giudiziaria ordinaria (Foro di Palermo con espressa rinuncia di qualsiasi altro).

Art. 11

(*Designazione del responsabile del trattamento dei dati personali*)

In esecuzione della fornitura di cui al presente capitolato, la Ditta effettua trattamento di dati personali di titolarità dell'Ente.

In virtù di tale trattamento, le parti stipulano l'Accordo allegato (Allegato A) al fine di disciplinare oneri e responsabilità in osservanza del Regolamento metropolitano per l'attuazione delle norme in materia di protezione dei dati personali (di seguito anche "Regolamento metropolitano"), del D.lgs. 30 giugno 2003, n. 1961, Codice in materia di protezione dei dati personali ...omissis... (di seguito, anche "Codice"), del Regolamento (UE) del Parlamento e del Consiglio europeo n. 2016/679 (di seguito, anche "RGDP") e di ogni altra normativa applicabile.

La Ditta è, pertanto, designata dalla Città Metropolitana di Palermo quale Responsabile del trattamento dei dati personali ai sensi e per gli effetti dell'art. 28 del RGDP e dell'art. 10 del Regolamento metropolitano, per il trattamento denominato "Gestione software uffici provinciali e scolastici" la quale si obbliga a dare esecuzione al contratto suindicato conformemente a quanto previsto dall'Accordo allegato al presente capitolato.

Le parti riconoscono e convengono che il rispetto delle istruzioni, di cui all'accordo allegato, nonché alle prescrizioni della normativa applicabile, non producono l'insorgere di un diritto in capo al Responsabile del trattamento al rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per conformarsi.

Allegato A

Accordo per il trattamento di dati personali

Il presente accordo allegato costituisce parte integrante del contratto siglato tra la Città metropolitana di Palermo e *il Fornitore* dei servizi operativi a supporto per il consolidamento ed evoluzione del prodotto EDR open-source Wazuh attualmente in uso presso l'amministrazione, designato Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del RGDP e dell'art. 10 del Regolamento metropolitano.

1. Premesse

Il presente accordo si compone delle clausole di seguito rappresentate e dai successivi allegati, anch'essi parti integranti e sostanziali dell'atto:

- allegato a: Glossario
- allegato b: Appendice "Security"

Le Parti convengono quanto segue:

2. Trattamento dei dati nel rispetto delle istruzioni della Città metropolitana di Palermo

2.1 Il Fornitore, relativamente a tutti i dati personali che tratta per conto dell'Ente garantisce che:

- tratta tali dati solo ai fini dell'esecuzione dell'oggetto del contratto e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto esclusivamente sulla base delle istruzioni documentate e fornite dall'Ente;
- non trasferisce i dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolte dall'Ente e a fronte di quanto disciplinato nel presente accordo;
- non tratta o utilizza i dati personali per finalità diverse da quelle per cui è conferito l'incarico dall'Ente, financo per trattamenti aventi finalità compatibili con quelle originarie;
- prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà l'Ente se, a suo parere, una qualsiasi istruzione fornita dall'Ente si ponga in violazione della normativa applicabile.

2.2. Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Fornitore si obbliga ad adottare:

- procedure idonee a garantire il rispetto dei diritti e delle richieste formulate all'Ente dagli interessati relativamente ai loro dati personali;
- procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta dell'Ente, dei dati personali di ogni interessato;
- procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta dall'Ente;

- procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dell'Ente.

2.3 Il Responsabile del trattamento deve garantire e fornire all'Ente cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dall'Ente, per consentirgli di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto dall'art. 30 del RGDP, deve mantenere, compilare e rendere disponibile a richiesta della Città metropolitana, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto *ex* artt. 35 del RGDP e 18 del Regolamento metropolitano che l'Ente intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve conservare i dati personali garantendo la separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto.

3.2 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.

3.3 Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

3.4 L'Ente attribuisce al Responsabile del trattamento il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti all'Ente, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.6 Il Responsabile del trattamento adotta le misure di sicurezza di cui all'Appendice "Security" allegata al presente accordo. In ragione della riservatezza delle evidenze di analisi di conformità alle misure di cui alla suddetta Appendice, il Fornitore condivide con l'Ente tali informazioni solo in caso di violazione o *data breach*. Si sottolinea che, ad ogni buon conto, la sottoscrizione del presente accordo, e dei suoi allegati, equivale ad attestazione della conformità del Responsabile, e della soluzione informatica prodotta/sviluppata, alle misure indicate nell' appendice "Security".

3.7 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle politiche dell'Ente in materia di privacy e sicurezza informatica, ed eventuali successivi aggiornamenti delle medesime policy. Le stesse sono consegnate a seguito della firma del presente accordo.

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dall'Ente sui trattamenti di dati personali cui concorre il Fornitore, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dall'Ente per affrontare eventuali rischi identificati.

4.2 Il Fornitore dovrà consentire all'Ente, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, garantendo in particolare che non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle politiche di privacy by design e by default adottate dall'Ente e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto dell'Ente.

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando all'Ente le evidenze di tale formazione.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel Contratto di cui il presente documento costituisce parte integrante. In ogni caso, il Fornitore sarà direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Il Fornitore, nell'eventualità di subappalto occorso ai sensi della normativa in materia di appalti e, per tutte le evenienze, nei casi di conferimento di parte del trattamento dei dati personali a soggetti terzi sub-responsabili, impone agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo.

6.2 Su specifica richiesta dell'Ente, il Fornitore dovrà provvedere a che ogni Sub-Responsabile sottoscriva direttamente con l'Ente un accordo di trattamento dei dati che,

a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente Accordo.

6.3 In tutti i casi, il Fornitore si assume la responsabilità nei confronti dell'Ente per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il Fornitore abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali fuori dall'area economica europea

7.1 L'Ente non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Fornitore provvede alla cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dall'Ente, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

8.2 Alla cessazione del Contratto, e conseguentemente del presente Accordo, per qualsiasi causa avvenga, i dati personali dovranno, a discrezione dell'Ente, essere distrutti o restituiti allo stesso, unitamente a qualsiasi supporto fisico o documento contenente dati personali di proprietà dell'Ente.

9. Audit

9.1 Il Fornitore si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte dell'Ente.

9.2 Il Fornitore consente, pertanto, all'Ente l'accesso ai propri locali e ai locali di qualsiasi Sub-Responsabile, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il Fornitore, e/o i suoi Sub-fornitori, rispettino gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, da questo Accordo.

9.3 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

9.4 Nel caso in cui l'audit fornisca evidenze di violazioni alla normativa in materia di protezione dei dati personali e al presente Accordo, quali ad esempio quelle indicate all'art. 83 comma 5 del RGDP (con esclusione della lett. e)), l'Ente può risolvere il Contratto o chiedere una cospicua riduzione del prezzo.

9.5 Nel caso in cui l'audit fornisca evidenze di violazioni gravi, quali ad esempio quelle indicate all'art. 83 comma 4 lett. a) del RGDP, l'Ente può chiedere una cospicua riduzione del prezzo.

9.6 Il rifiuto del Fornitore di consentire l'audit all'Ente comporta la risoluzione del contratto.

10. Indagini dell'Autorità e reclami

Nei limiti della normativa applicabile, il Fornitore o qualsiasi Sub-Responsabile informa senza alcun indugio l'Ente di qualsiasi:

- richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine;
- istanza ricevuta da soggetti interessati.

Il Fornitore fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza all'Ente per garantire che la stessa possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 Il Fornitore, in virtù di quanto previsto dall'art. 33 del RGDP, dovrà comunicare a mezzo di posta elettronica certificata all'Ente nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato 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, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach,* oltre a:

- descrivere la natura della violazione dei dati personali;
- le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- i recapiti del DPO nominato o del soggetto competente alla gestione del *data breach*;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o che si intende adottare per affrontare la violazione della sicurezza, comprese, ove opportuno, misure per mitigare i suoi possibili effetti negativi.

11.2 Il Fornitore deve fornire tutto il supporto necessario all'Ente ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con l'Ente, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Fornitore non deve rilasciare né pubblicare alcun comunicato stampa o relazione riguardante eventuali *data breach* o violazioni di trattamento senza aver ottenuto il previo consenso scritto dell'Ente.

12. Responsabilità e manleve

12.1 Il Fornitore tiene indenne e manleva l'Ente da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o collegata a una qualsiasi violazione da parte del Fornitore delle disposizioni contenute nel presente accordo.

12.2 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente

Accordo, il Fornitore:

- avverte prontamente ed in forma scritta l'Ente del reclamo;
- non fornisce dettagli al reclamante senza la preventiva interazione con l'Ente;
- non transige la controversia senza il previo consenso scritto dell'Ente;
- fornisce all'Ente tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

Allegato a)

GLOSSARIO

***Garante per la protezione dei dati personali*:** è l'autorità di controllo responsabile per la protezione dei dati personali in Italia;

***Dati personali*:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

***RGDP* :** si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation), direttamente applicabile dal 25 maggio 2018;

***Codice*:** D.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali e ss.mm.ii., recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Regolamento metropolitano: il Regolamento metropolitano per l'attuazione delle norme in materia di protezione dei dati personali, adottato dal Consiglio metropolitano con delibera n. 137 in data 23 dicembre 2019;

***Normativa Applicabile*:** si intende l'insieme delle norme rilevanti in materia protezione dei dati personali , incluso il Regolamento Privacy UE 2016/679 (GDPR), il Codice in materia di protezione dei dati personali, D.lgs. n. 196/2003 e ss.mm.ii. recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento Ue 2016/679 ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

***Appendice Security*:** consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, che possono dallo stesso essere aggiornate ed implementate di volta in volta, in conformità alle previsioni del presente Accordo;

***Reclamo*:** si intende ogni azione o segnalazione presentata nei confronti del Titolare o di un suo Responsabile del trattamento;

***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 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;

Trattamento**:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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 di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Pseudonimizzazione**:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Allegato b)

Appendice *Security*

L’Ente deve adottare le misure minime per la sicurezza ICT stabilite da AGID con la circolare del 18 aprile 2017, n. 2 pubblicata sulla Gazzetta Ufficiale, al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi. Tali misure sono descritte all’indirizzo: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict