Contratto tramite Trattativa Diretta sul MePA ai sensi dell'art. 50, comma 1 lett. b) del D.lgs. n. 36/2023, per garantire l'acquisizione di servizi di Cybersecurity per il CERT-AgID necessari alla sicurezza informatica dell'Agenzia per l'Italia Digitale.

INDICE

Contratto tramite trattativa diretta su MePA, ai sensi dell'art. 50, comma 1 lett. b) del d.lgs. n. 36/2023, per garantire l'acquisizione di servizi di Cybersecurity per il CERT-AgID necessari alla sicurezza informatica dell'Agenzia per l'Italia Digitale.

TRA

Agenzia per l'Italia Digitale (AgID), con sede in Roma, Via Liszt n. 21, C.F. 97735020584, nella persona del Direttore generale Mario Nobile incarico conferito con D.P.C.M. del 23 marzo 2023, a firma del Sottosegretario per l'innovazione tecnologica e la digitalizzazione Sen. Alessio Butti, registrato dalla Corte dei Conti in data 3 aprile 2023 al n. 945, ai sensi dell'art.21, comma 2, del decreto legge 22 giugno 2012 n.83, convertito con modificazioni dalla legge 7 agosto 2012 n.134 (nel seguito per brevità anche "AgID" o "Agenzia"),

E

La Società D3Lab s.r.l., con sede a Cecina (LI) - Via Petrarca 18, P. IVA IT01865450496,

PREMESSO che:

- L'Agenzia per l'Italia Digitale (AgID) è il soggetto istituzionale che ha il compito di coordinare il processo di attuazione del Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026, all'interno del quale una delle principali linee strategiche è costituita dalla Sicurezza informatica;
- il Piano Triennale, al punto 7.6 della Sicurezza Informatica, ha previsto che AgID metta a disposizione della Pubblica Amministrazione una serie di piattaforme e di servizi, che verranno erogati tramite il proprio CERT, finalizzati alla conoscenza e al contrasto dei rischi cyber legati al patrimonio ICT della PA;
- questi servizi comprendono tra gli altri le attività di monitoraggio e identificazione delle minacce presenti sui canali underground che potrebbero interessare la constituency del CERT-AGID e, più in generale, il dominio della PA nazionale, anche attraverso attività di ricerca in ambito di Cyber Threat Intelligence, Data Leak, Malware, Phishing e condivisione di Indicatori di Compromissione **(IoC Phish Leak CTI);**
- il CERT-AgID, che già svolge parte di queste attività, ha necessità di potenziarle ampliando la qualità di informazioni da mettere a disposizione della PA, sia dal punto di vista della quantità sia da quello della completezza, potendo avere accesso ad altre fonti informative complementari a quelle attuali;
- alla luce delle verifiche e indagini di mercato condotte, è stato riscontrato che l'Operatore Economico D3Lab Srl, con sede a Cecina (LI) - Via Petrarca 18, P. IVA IT01865450496, presente sul MePA, propone, nelle righe di catalogo, l'insieme dei servizi essenziali alla sicurezza delle infrastrutture dell'Agenzia;
- è stata indetta apposita Trattativa diretta su MePA, ai sensi dell'art. 50, comma 1 lett. b) del d.lgs. n. 36/2023, per garantire l'acquisizione dei servizi di Cybersecurity per il CERT-AgID per un periodo di 24 mesi, a decorrere dalla stipula del contratto, e per l'importo complessivo massimo di Euro 70.000,00 IVA esclusa, pari ad Euro 85.400,00 IVA inclusa;
- è stato acquisito il CIG;
- a seguito della TD è stata formulata l'offerta su MePA;
- a seguito della verifica positiva della documentazione presentata, della verifica del possesso dei requisiti dell'operatore economico risultato aggiudicatario ai sensi degli art. 94 e 95 del D.lgs. n. 36/2023 si procede alla stipula su MePA;

TUTTO CIO' PREMESSO SI STIPULA QUANTO SEGUE

ART.1 CONTESTO TECNICO, OBIETTIVI ATTESI. OGGETTO, IMPORTO, DURATA, CONTENUTI DELL'AFFIDAMENTO.

1.Alla luce del contesto sinteticamente richiamato anche in premessa e degli obiettivi da realizzare, l'Agenzia si è garantita l'acquisizione, per un periodo di 24 mesi a decorrere dalla stipula del contratto e per l'importo complessivo massimo di Euro 70.000,00 IVA esclusa, pari ad Euro 85.400,00 IVA inclusa, dei servizi di Cybersecurity per il CERT-AgID, legati ad attività di ricerca in ambito di Cyber Threat Intelligence, Data Leak,

Malware, Phishing e condivisione di Indicatori di Compromissione contenuti nel pacchetto **IoC Phish Leak CTI,** di seguito indicati:

Servizio	Descrizione	Durata
Phishing Monitor	Servizio per individuare il diffondersi di frodi on-line della tipologia phishing miranti a carpire dati personali, sensibili e finanziari di utenti finali o del personale in servizio presso il cliente.	24 Mesi
Brand Monitor	Monitoraggio delle diverse tecniche di typosquatting applicate ai domini istituzionali. In particolare identifica i domini di nuova registrazione aventi nomi sospetti e similari ai brand/domini del cliente che potrebbero essere impiegati per: • rivendita/cessione speculativa del nome dominio; • phishing utenza customers; • spear-phishing: phishing mirato all'organizzazione del cliente; • attacco all'immagine del cliente, con la pubblicazione di false notizie.	24 Mesi
Data Leak/Breach Monitor	Servizi di: • Data Leak Monitor: monitoraggio degli ambienti underground al fine di rilevare il rilascio di dati estrapolati da siti web di qualsiasi dimensione in cui i dipendenti si siano registrati con l'indirizzo email aziendale, con il rischio di riutilizzo sui sistemi aziendali della medesima password; • Recupero Email da Phishing: deputato a recuperare gli indirizzi email di coloro che cadono vittime di phishing a danno di qualsiasi tipologia di ente.	24 Mesi
CTI Main Core	Attività di monitoraggio dei contenuti presenti sul Web: • monitoraggio automatizzato delle piattaforme accessibili sul web emerso, attraverso connettori sviluppati ad hoc per collegare le sorgenti di informazioni alla Threat Intelligence Platform; • frequentazione dagli ambienti underground/cyber criminali, identificabili in Deep e Dark web, da parte dell'operatore del fornitore facendo uso di profili ad hoc (sock puppets) credibili.	24 Mesi
IoC Zone	Servizio finalizzato alla condivisione di indicatori di compromissione (IoC) derivanti dall'analisi statica ed in sandbox dei malware per sistemi desktop e mobili, identificati attraverso la raccolta su apposite spamtrap gestite ed attraverso i monitoraggi web svolti con automatismi e ricerche condotte da operatori.	24 Mesi

3.Il Fornitore dovrà garantire, per tutta la durata del servizio, il necessario supporto per tutti gli aspetti operativi e svolgere le attività nel rispetto delle specifiche di dettaglio presenti nell'**Allegato** e delle direttive del RUP.
4.Ai fini della stipula della trattativa diretta, il fornitore dovrà prestare, ai sensi dell'art. 53 comma 4 del D.lgs. n. 36/2023, una garanzia fideiussoria, come precisato anche nel prosieguo all'**art. 2**.
5.Data la tipologia dei servizi acquisiti, l'OE sarà nominato responsabile del trattamento dei dati personali ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 2016/679.

ART.2 GARANZIA DEFINITIVA

1.Ai fini della stipula della trattativa diretta su MePA, il fornitore dovrà prestare, una garanzia fideiussoria ai sensi dell'art. 53, comma 4 del D.lgs. 36/2023, da rilasciare con le modalità indicate nel codice.
2.La garanzia deve contenere la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, comma 2, del codice civile, l'operatività della garanzia medesima -anche per il recupero delle penali contrattuali - entro quindici giorni, a semplice richiesta scritta della Amministrazione contraente.
3.Deve essere munita, in deroga all'art. 1945 del codice civile, della clausola "a prima richiesta" con espressa rinuncia, altresì, alla preventiva escussione del debitore principale di cui all'art. 1944 del codice civile.
4.Al fine di fruire del beneficio della riduzione previsto dall'art. 106, comma 8 del D.lgs. n. 36/2023, il Fornitore deve produrre, anche in copia conforme all'originale, mediante idonea dichiarazione resa ai sensi dell'art. 47del D.P.R. 445/2000, la certificazione di qualità conforme alle norme europee UNI CEI ISO 9000; ovvero rientrare in tutte le altre ipotesi indicate nel codice dei contratti.

5. Si precisa che:
- in caso di partecipazione in R.T.I. e/o Consorzio ordinario di cui all'art. 65, comma 2, lett. e) del D.lgs. 36/2023, il Fornitore può godere del beneficio della riduzione della garanzia solo se tutte le imprese che lo costituiscono siano in possesso della predetta certificazione, attestata da ciascuna impresa secondo le modalità sopra previste;
- in caso di partecipazione in Consorzio di cui alle lettere b), c) e d) dell'art. 65, comma 2, del D.lgs.36/2023, il Fornitore può godere del beneficio della riduzione della garanzia solo se il Consorzio è in possesso della predetta certificazione.

6.Qualora l'ammontare delle garanzie dovesse ridursi per effetto dell'applicazione di penali, o per qualsiasi altra causa, l'affidatario dovrà provvedere al reintegro entro il termine di 30 (trenta) giorni lavorativi dal ricevimento della relativa richiesta. In caso di inadempimento al reintegro, la Stazione Appaltante ha facoltà di dichiarare risolto il contratto, fermo restando il risarcimento del danno.

7.La mancata costituzione della garanzia definitiva determina l'impossibilità di stipulare e la decadenza dall'affidamento. La cauzione copre gli oneri per il mancato od inesatto adempimento dell'appalto e cessa di avere effetto a completa ed esatta esecuzione delle obbligazioni nascenti dallo stesso.

8.Si ricorda che la garanzia è progressivamente svincolata in ragione e a misura dell'avanzamento dell'esecuzione, nel limite massimo dell'80% dell'iniziale importo garantito secondo quanto stabilito all'art. 117, comma 8, D.lgs. 36/2023.

Art.3 ADEMPIMENTI CONNESSI ALLA STIPULA E ALLA ESECUZIONE DELL'AFFIDAMENTO

1.A seguito dell'affidamento sulla piattaforma elettronica, si richiede, come in parte già chiarito, di far pervenire all'indirizzo PEC: protocollo@pec.agid.gov.it, all'attenzione del RUP e del Direttore dell'esecuzione e all'Ufficio Contabilità, Finanza e Funzionamento entro il termine di 10 (dieci) giorni naturali e consecutivi la prova del pagamento dell'imposta di bollo che l'appaltatore è tenuto a versare al momento della stipula del contratto secondo l'articolo 1, comma 1, dell'allegato I.4 al d.lgs. n. 36/2023. I contratti stipulati con la Pubblica Amministrazione attraverso il Mercato Elettronico della PA scontano l'imposta di bollo, in linea anche con la risoluzione n. 37/E del 28 giugno 2023 dell'Agenzia delle Entrate.

2.Le modalità di versamento utilizzabili per assolvere l'imposta di bollo sui contratti pubblici, così come rideterminata nel valore, in funzione delle fasce di importo del contratto, dalla tabella A dell'articolo 3 del citato Allegato I.4, prevedendo l'utilizzo del diffuso sistema di pagamento F24. Tale strumento è idoneo a consentire, da un lato, il versamento in via telematica attraverso gli appositi servizi messi a disposizione dall'Agenzia delle entrate, dalle banche e dagli altri prestatori di servizio di pagamento e, dall'altro, mediante utilizzo dello specifico modello "F24 ELIDE", ad assicurare la possibilità di un'univoca associazione del versamento stesso con il contratto soggetto ad imposta, mediante la valorizzazione del campo elementi identificativi (con l'indicazione del CIG o di altro identificativo univoco).

3.Il RUP principalmente e nel rispetto delle norme vigenti:
- cura il corretto e razionale svolgimento della procedura su MePA, esercitando una funzione di coordinamento e controllo anche sulla documentazione da inviare tramite piattaforma (e coordinandosi con il punto ordinante e i servizi competenti) adottando decisioni conseguenti alle valutazioni effettuate;
- verifica, ove lo ritenga necessario anche con il supporto degli uffici competenti, il possesso dei requisiti previsti dal Codice e dalle altre disposizioni vigenti in capo all'aggiudicatario e il costante mantenimento dei requisiti e adempimenti essenziali a garantire il rispetto della normativa in tema di GDPR e la sicurezza informatica;
- richiede al punto ordinante di procedere attraverso le funzionalità del MePA alla stipula del contratto (se vi sono urgenze di avvio del servizio, anche una volta avviate le verifiche di cui al precedente punto);
- comunica al Prestatore e agli Uffici competenti, anche ai fini degli adempimenti legati alla normativa in materia di trasparenza e avvio della fase di gestione, controllo, esecuzione, pagamento dei servizi resi in forza del contratto, la data di avvio delle attività;
- rilascia l'Attestazione di regolare esecuzione (ARE)/il certificato di pagamento, entro i termini previsti

d e lo invia all'OE e all'ufficio competente, ai fini dell'autorizzazione alla fatturazione e per il pagamento, previa ricezione della fattura, coerente con l'ARE.

3.1 Garanzia dell'esatto adempimento

A garanzia dell'esatto e tempestivo adempimento degli obblighi contrattuali di cui al presente Contratto, il Fornitore garantisce le obbligazioni assunte con il presente contratto, il risarcimento dei danni derivanti dall'eventuale inadempimento delle stesse obbligazioni, salva comunque la risarcibilità del maggior danno verso l'appaltatore, nonché, ove esistente, le obbligazioni assunte con il Patto di integrità.

ART.4 PENALI E RISOLUZIONE

1.In caso di ritardo rispetto ai termini indicati dal RUP e in caso di inadempimento nell'erogazione dei servizi richiesti per assicurare tutti i servizi acquistati e previsti dal contratto, per ogni difetto contestato formalmente, anche via mail, il RUP si riserva di applicare una penale del'1‰ dell'importo contrattuale per ogni giorno solare di ritardo e per ogni inadempienza contestata.
2.L'ammontare della penale sarà detratto dal corrispettivo dovuto, salvo che il danno sia così grave da preludere alla risoluzione del contratto.
3.Le penali saranno applicabili fino ad un massimo del 10% (dieci per cento) dell'importo contrattuale.
4.Oltre tale limite, l'Agenzia si riserva la facoltà di risolvere il rapporto mediante PEC, senza bisogno di messa in mora o di azione giudiziaria, con rivalsa nei confronti della contraente anche dell'eventuale maggior onere rispetto alle condizioni economiche di cui alla presente procedura, salvo le richieste di risarcimento dei danni subiti.
5.Il protrarsi dell'inadempimento del contratto, costituisce condizione risolutiva espressa, ai sensi dell'art. 1456 cc., senza che l'inadempiente abbia nulla a pretendere, e fatta salva l'esecuzione in danno con facoltà dell'Agenzia di risolvere il rapporto mediante PEC, senza bisogno di messa in mora o di azione giudiziaria, con rivalsa nei confronti della contraente anche dell'eventuale maggior onere rispetto alle condizioni economiche di cui alla presente procedura e salvo le richieste di risarcimento dei danni subiti.
6.Resta in ogni caso salva la facoltà per l'AgID di richiedere il risarcimento di eventuali danni subiti a seguito di inadempienze verificatesi nel periodo di erogazione del servizio/fornitura.
7.Qualora nell'arco della durata del contratto dovessero registrarsi inadempienze con frequenza ritenuta eccessiva dall'Agenzia, quest'ultima potrà in ogni momento, a proprio insindacabile giudizio, considerare risolto di diritto il contratto, in danno e per colpa del Prestatore, ovvero acquisendo anche i prodotti in danno dell'OE da altro fornitore, ferma restando la facoltà dell'Agenzia stessa di richiedere danni diretti e indiretti derivanti dalla risoluzione.
8.L'Agenzia, inoltre, procederà alla risoluzione del contratto, in danno e colpa del Prestatore, in caso di:

- frode o grave negligenza nell'esecuzione degli obblighi e delle condizioni contrattuali;
- circostanze, determinatesi per colpa del Prestatore, tali da rendere impossibile la prosecuzione dei rapporti fra le parti;
- cessione contratto, cessazione attività, concordato preventivo, fallimento.

ART.5 ATTESTAZIONE/CERTIFICATI DI REGOLARE ESECUZIONE DEI SERVIZI. TERMINI E MODALITÀ DI FATTURAZIONE E PAGAMENTO.

1.Il servizio e quanto richiesto al Prestatore entro i termini indicati, saranno oggetto di verifica di conformità e funzionalità da parte del RUP. L'importo sarà liquidato solo a seguito dell'attestazione di regolare esecuzione del RUP e previa verifica di conformità positiva del servizio di Cybersecurity.
2.Il pagamento dell'importo è in ogni caso subordinato alla stipula del contratto e sarà effettuato entro 30 (trenta) giorni dalla data di presentazione della fattura. La fattura potrà essere emessa solo successivamente all'attestazione di regolare esecuzione del RUP
3. La fattura pervenuta prima dell'attestazione di regolare esecuzione è passibile di rifiuto da parte dell'AgID.
4.Il Prestatore dovrà produrre esclusivamente fatture elettroniche, in ottemperanza a quanto previsto dal D.M. n. 55 del 3 aprile 2013, così come integrato dal Decreto del 24 agosto 2020, n. 132 del Ministero

dell'Economia e delle Finanze, inerente il "*Regolamento recante individuazione delle cause che possono consentire il rifiuto delle fatture elettroniche da parte* delle *amministrazioni pubbliche. (20G00148) (GU n.262 del 22-10-2020)*".

5.L'AgID sarà costretta a procedere al rifiuto delle fatture:

a) riferite ad una operazione che non è stata posta in essere in favore del soggetto destinatario della trasmissione;

b) in caso di omessa o errata indicazione del Codice identificativo di Gara (CIG) o del Codice unico di Progetto (CUP), da riportare in fattura ai sensi dell'articolo 25, comma 2, del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89;

c) che non rispettino le norme del codice in tema di verifica di conformità e contenuti e non consentano la comprensione del contratto o progetto cui si riferiscono.

6.Sono elementi essenziali della fattura ai fini dei precedenti punti a), b) e c) i seguenti:

- Denominazione Ente: Agenzia per l'Italia Digitale;
- Codice Univoco Ufficio: F7VRDL;
- C.F.: 97735020584;
- i riferimenti (protocollo e data) della lettera contratto di affidamento del servizio e/o della fornitura e alla determinazione a contrarre e di copertura di budget;
- il CIG (Codice Identificativo Gara), in base all'art 25 c. 2 del D.L. n. 66/2014 (convertito dalla L. 23 giugno 2014, n. 89);
- i riferimenti al progetto e al CUP se presenti;
- la descrizione del servizio o della fornitura cui la fattura fa riferimento;
- la "competenza temporale del servizio", l'anno cui si riferisce il costo del servizio/fornitura (es. dal gg/mm/aa …… al gg/mm/aa….); ovvero il periodo (gg.mm.aa.) di erogazione del servizio/di effettuazione della fornitura, nonché tutti gli elementi utili alla comprensione degli importi unitari e totali che hanno condotto all'importo fatturato (limitando il più possibile il ricorso a documenti collegati);
- tutti gli elementi utili alla comprensione degli importi unitari e totali che hanno condotto all'importo fatturato (limitando il più possibile il ricorso a documenti collegati);
- eventuale titolo di non imponibilità o esenzione IVA;
- l'indicazione dello split payment;
- l'esposizione in fattura delle ritenute dello 0,50% di cui all'art. 11, comma 6 del D.lgs. n. 36/2023.

Split payment: Come detto, AgID, ai sensi del D.L. n. 50/2017 del 24/04/2017 "*Disposizioni urgenti in materia finanziaria, iniziative a favore degli enti territoriali, ulteriori interventi per le zone colpite da eventi sismici e misure per lo sviluppo*", è compresa nella platea dei destinatari del meccanismo della scissione dei pagamenti (split payment) previsto dall'articolo 1, comma. 629, lettera b), della legge 23 dicembre 2014, n. 190. L'Agenzia provvederà a versare direttamente all'Erario l'IVA addebitata in fattura, pagando al fornitore esclusivamente l'imponibile. La fattura elettronica, nella sezione "Dati di riepilogo per aliquota IVA e natura" dovrà contenere, alla voce: "Esigibilità IVA" l'indicazione: "S (scissione dei pagamenti)". Fatture non conformi a quanto indicato sono passibili di rifiuto tramite lo SDI (Sistema di Interscambio) dell'Agenzia delle Entrate.

ART.6 OBBLIGHI DI TRACCIABILITÀ

1.L'operatore economico assume gli obblighi di tracciabilità dei flussi finanziari di cui alla legge 13 agosto 2010, n. 136 e ss.mm.ii., "Piano straordinario contro le mafie". Pertanto lo stesso deve comunicare all'Agenzia gli estremi identificativi dei conti correnti bancari o postali dedicati; la comunicazione deve essere effettuata entro sette giorni dall'accensione del conto corrente ovvero, nel caso di conti correnti già esistenti, dalla loro prima utilizzazione in operazioni finanziarie relative ad una commessa pubblica.

In caso di persone giuridiche, la comunicazione de quo deve essere sottoscritta da un legale rappresentante ovvero da un soggetto munito di apposita procura.

2.L'omessa, tardiva o incompleta comunicazione degli elementi informativi comporta, a carico del soggetto inadempiente, l'applicazione di una sanzione amministrativa pecuniaria.

3.Il mancato adempimento agli obblighi previsti per la tracciabilità dei flussi finanziari relativi all'appalto comporta la risoluzione di diritto del contratto. In occasione di ogni pagamento all'operatore economico o di interventi di controllo ulteriori si procede alla verifica dell'assolvimento degli obblighi relativi alla tracciabilità dei flussi finanziari.
4.Il contratto è sottoposto alla condizione risolutiva in tutti i casi in cui le transazioni siano state eseguite senza avvalersi di banche o di Società Poste Italiane S.p.a. o anche senza strumenti diversi dal bonifico bancario o postale che siano idonei a garantire la piena tracciabilità delle operazioni per il corrispettivo dovuto in dipendenza del presente contratto.

ART.7 RISERVATEZZA

L'operatore economico si impegna formalmente a dare istruzioni al proprio personale affinché tutti i dati e le informazioni patrimoniali, statistiche, anagrafiche e/o di qualunque altro genere di cui verrà a conoscenza in conseguenza dei servizi resi vengano considerati riservati e come tali trattati, pur assicurando nel contempo la trasparenza delle attività svolte.

ART.8 OBBLIGHI IN MATERIA DI PREVENZIONE DELLA CORRUZIONE

1.AgID informa la propria attività contrattuale secondo i contenuti di cui al Codice di Comportamento approvato con Determinazione del Direttore Generale n. 21 del 30 gennaio 2015 (aggiornata con Determinazione n. 13 del 18/01/2023) quale dichiarazione dei valori, insieme dei diritti, dei doveri e delle responsabilità, nei confronti dei portatori di interesse (dipendenti, fornitori, utenti, ecc.), in ottemperanza a quanto previsto dall'art. 54 del D.lgs.
n. 165/2001 così come sostituito dall'art. 1, comma 44 della L. 190/2012 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica Amministrazione", documento che integra e specifica il Codice di Comportamento dei dipendenti pubblici di cui al DPR n. 62/2013.
2.Le norme contenute nel Codice si applicano, per quanto compatibili, ai titolari di contratti di consulenza o collaborazione a qualsiasi titolo, anche professionale, ai titolari di organi e di incarichi negli uffici di diretta collaborazione dei vertici politici dell'amministrazione, nonché ai collaboratori a qualsiasi titolo, anche professionale, di imprese fornitrici di servizi in favore dell'Agenzia.
3.L'operatore economico affidatario quale soggetto terzo è tenuto, nei rapporti con AgID, ad uniformare la propria condotta ai criteri fondati sugli aspetti etici della gestione dei contratti definiti nel Codice di Comportamento, tenendo presente che la violazione dello stesso comporterà la risoluzione di diritto del rapporto contrattuale in essere, nonché il pieno diritto di AgID di chiedere ed ottenere il risarcimento dei danni patiti per la lesione della sua immagine ed onorabilità.

Art.9. DESIGNAZIONE AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679

1. Con la sottoscrizione del presente Contratto, l'Agenzia per l'Italia Digitale, in qualità di titolare del trattamento dei dati personali, designa l'OE quale responsabile del trattamento ai sensi e per gli effetti degli artt. 4, n. 8) e 28 del Regolamento (UE) 2016/679, con riferimento alle attività oggetto del presente Contratto.
2. Il trattamento dei dati personali è così individuato:

- Oggetto: Servizi anti-phishing e legati all'attività di ricerca di minacce Cyber presenti su canali underground e non, in ambito di Cyber Threat Intelligence, Data Leak, Malware e condivisione di Indicatori di Compromissione;
- Durata: sino all'esecuzione delle attività di cui alla Contratto o, in ogni caso, sino alla scadenza del Contratto;
- Finalità: Monitoraggio proattivo delle minacce cyber nel dominio della PA, funzionale alla diffusione di Indicatori di Compromissione e informazioni utili all'innalzamento del livello di difesa e allo sviluppo di servizi di sicurezza preventivi oltre a funzioni di accompagnamento utili per la crescita e la diffusione della cultura della sicurezza informatica;
- Tipologia di dati personali trattati: dati comuni (es. nome, cognome, indirizzo mail, dati di contatto, ecc.), categorie particolari di dati personali e dati giudiziari;

- Categorie di interessati: qualsiasi utente pubblico o privato, i cui dati personali siano stati coinvolti in campagne malevole online.

3. Per la durata del Contratto e per le attività in esso disciplinate, il responsabile del trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, della tipologia di dati personali trattati, delle categorie di interessati nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, si impegna nei confronti del Titolare a:

- trattare i dati personali nel rispetto dei princìpi e delle disposizioni previsti dal Regolamento (UE) 2016/679, dal D. Lgs. 196/2003 e s.m.i., dagli indirizzi e dai provvedimenti a carattere generale emanati dallo European Data Protection Board e dal Garante per la protezione dei dati personali e da ogni altra vigente normativa in materia di protezione dei dati personali;
- trattare i dati personali, acquisiti nello svolgimento delle attività delegate, per le sole finalità di cui al Contratto;
- nel trattare i dati personali, attenersi alle istruzioni fornite dall'Agenzia, anche in caso di eventuale trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o la normativa nazionale; in tal caso, il responsabile del trattamento si impegna a informare l'Agenzia circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico. Sono considerate istruzioni le prescrizioni previste dal Contratto, le indicazioni di cui all'eventuale valutazione d'impatto sulla protezione dei dati personali laddove svolta ai sensi di legge e periodicamente revisionata, la presente designazione, le regole tecniche e le linee guida emanate dall'Agenzia, laddove applicabili, e ogni altra eventuale comunicazione inoltrata dall'Agenzia al responsabile e concernente le modalità di trattamento dei dati. Il responsabile informerà l'Agenzia qualora ritenga che un'istruzione impartitagli da quest'ultima violi il Regolamento (UE) 2016/679 o altre disposizioni unionali europee o nazionali relative alla protezione dei dati; − non trasferire, né in tutto né in parte, in un Paese terzo o a un'organizzazione internazionale i dati personali trattati ai sensi del Contratto, senza la previa autorizzazione dell'Agenzia, e limitarsi alle sole comunicazioni strettamente necessarie alle finalità di cui al Contratto;
- ai sensi dell'art. 30, par. 2 del Regolamento, tenere il registro delle attività relative al trattamento dei dati personali effettuate per conto dell'Agenzia e, su richiesta, mettere tale registro a disposizione dell'Agenzia stessa e/o del Garante per la protezione dei dati personali;
- formare adeguatamente i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali, ai sensi dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del D. Lgs. 196/2003 e s.m.i. e garantire che su questi gravi un adeguato obbligo legale di riservatezza;
- tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, adottare le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del Regolamento (UE) 2016/679. Nel caso in cui il trattamento, per la propria natura, il contesto e/o le tecnologie utilizzate, evidenziasse la necessità di approntare ulteriori misure di sicurezza, l'Agenzia potrà richiedere al responsabile l'implementazione di tali misure. Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista dal Contratto e le misure di sicurezza richieste, il responsabile si impegna a comunicarlo per scritto all'Agenzia, fornendo alla medesima l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate;
- fornire supporto all'Agenzia, qualora richiesto, nell'effettuazione della valutazione d'impatto sulla protezione dei dati personali;
- consentire all'Agenzia l'effettuazione di verifiche periodiche, ispezioni e/o audit circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate e il pieno e scrupoloso rispetto delle norme in materia di protezione dei dati personali;
- avvisare l'Agenzia tempestivamente e senza ingiustificato ritardo in caso di ispezioni, di richiesta di

informazioni e di documentazione da parte del Garante per la protezione dei dati personali e assistere l'Agenzia in tali contesti;

- informare l'Agenzia, tempestivamente e senza ingiustificato ritardo, di ogni violazione di dati personali, condividendo ogni documentazione utile e assistendo l'Agenzia nella gestione della violazione e, qualora necessario, nella relativa notifica al Garante per la protezione dei dati personali entro il termine di 72 ore dall'intervenuta conoscenza della violazione nonché nell'eventuale comunicazione agli interessati, ai sensi degli artt. 33 e 34 del Regolamento (UE) 2016/679;
- assistere l'Agenzia nell'adempimento dei propri obblighi derivanti dall'esercizio, da parte degli interessati, dei diritti di cui al Capo III del Regolamento (UE) 2016/679;
- ricorrere a un altro responsabile (di seguito sub-responsabile) esclusivamente qualora quest'ultimo offra garanzie sufficienti alla messa in atto di misure di sicurezza tecniche e organizzative adeguate ai sensi del Regolamento (UE) 2016/679 e solo previa autorizzazione scritta dell'Agenzia. Il responsabile dovrà comunicare tempestivamente all'Agenzia i dati identificativi del sub-responsabile, i dati del contratto di esternalizzazione e le attività di trattamento delegate, nonché la decadenza o sostituzione del sub-responsabile. Ogniqualvolta l'Agenzia autorizzi il ricorso del responsabile a un sub-responsabile per l'esecuzione di specifiche attività di trattamento, a quest'ultimo sono imposti, mediante la stipula di un contratto o altro atto giuridico sottoscritto dal responsabile e dal sub-responsabile stesso, i medesimi obblighi in materia di protezione dei dati personali contenuti nella presente designazione. Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile conserva, nei confronti dell'Agenzia, l'intera responsabilità dell'adempimento di tali obblighi; − mettere a disposizione dell'Agenzia tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui alla presente designazione ai sensi dell'art. 28 del Regolamento (UE) 2016/679 e consentire e contribuire alle attività di revisione, comprese le ispezioni, eseguite dall'Agenzia o da altro soggetto da questi incaricato;
- su richiesta dell'Agenzia, cancellare o restituire alla medesima tutti i dati personali al termine del Contratto o comunque della prestazione dei servizi relativi al trattamento nonché cancellare le copie esistenti, salvo che il diritto dell'Unione europea o la normativa nazionale prevedano la conservazione dei dati.

4. Per quanto non espressamente previsto dalla presente designazione, si fa espresso riferimento alla normativa unionale e nazionale in materia di protezione dei dati personali.

ART.10 CODICE DI COMPORTAMENTO/PATTO DI INTEGRITÀ

1.L'operatore economico dovrà altresì attenersi al D.P.R. 16 aprile 2013, n. 62 (Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del D.lgs. n. 30 marzo 2001, n. 165), come modificato dal D.P.R. 13 giugno 2023, n. 81, in particolare dall'art. 2, co.3, alla cui stregua le PP.AA. estendono gli obblighi di condotta previsti dal codice di comportamento anche nei confronti di imprese fornitrici di beni e servizi.

2.Nel caso di violazione degli obblighi derivante dal citato codice e sue ss.mm.ii., AgID potrà procedere alla risoluzione o decadenza del rapporto contrattuale. L'operatore economico affidatario dei servizi accetta inoltre sin d'ora quanto disposto nel PNA ANAC vigente e dai seguenti Piani e Determinazioni: il Piano Integrato di attività e organizzazione (PIAO) 2024 – 2026, adottato con la DT DG n. 28/2024 del 31 gennaio 2024; la DT DG n. 26/2024 del 31 gennaio 2024 di "Aggiornamento del Piano Triennale per la Prevenzione della Corruzione e della Trasparenza (PTPCT) 2024-2026.

3.In seguito alla comunicazione di affidamento e prima della stipula del contratto, l'operatore economico ha l'onere di prendere visione dei predetti documenti sul sito dell'Agenzia.

4.L'operatore economico, affidatario dei servizi si impegna a sottoscrivere e rispettare, infine, il Patto di integrità sottoposto da Consip e firmato in sede di abilitazione al Mercato Elettronico, nonché il Patto di integrità AgID di cui al relativo allegato.

ART.11 FORO COMPETENTE

Per tutte le controversie relative alla validità, interpretazione ed esecuzione delle clausole contrattuali e del presente documento integrativo è competente in via esclusiva il Foro di Roma.
Letto, approvato e sottoscritto (per l'operatore economico)

Ai sensi e per gli effetti dell'art. 1341 c.c. l'operatore economico dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli seguenti:
Art.1 Contesto tecnico, obiettivi attesi. oggetto, importo, durata, contenuti dell'affidamento;
Art.4 Penali e risoluzione;
Art.5 Attestazione/certificati di regolare esecuzione dei servizi. termini e modalità di fatturazione e pagamento;
Art.11 Foro competente.
(per l'operatore economico)

ALLEGATO: SPECIFICHE DI DETTAGLIO DEL PACCHETTO SERVIZI DENOMINATO "IoC Phish Leak CTI"

I servizi contenuti nel pacchetto denominato "IoC Phish Leak CTI" sono:
1. Phishing Monitor;
2. Brand Monitor;
3. Data Leak/Breach Monitor
4. CTI Main Core;
5. IoC Zone;

PHISHING MONITORING
Il servizio anti-phishing deve individuare il diffondersi di frodi on-line della tipologia phishing miranti a carpire dati personali, sensibili e finanziari di utenti finali/clienti del Cliente o del personale in servizio presso il Cliente. L'attività di monitoraggio è volta alla tempestiva individuazione dei soggetti, intesi quali computer, server e siti, coinvolti negli attacchi di phishing.
Tale attività dovrà essere svolta attraverso il monitoraggio, automatizzato e non, di:
- Messaggi di posta elettronica ricevuti su caselle di posta elettronica (spamtrap);
- Database di segnalazioni on-line;
- Monitoraggio attivo mediante l'analisi di altre segnalazioni;
- Monitoraggio di Social Network;
- Passive DNS;
- Phishing Feed gratuiti ed a pagamento;
- Monitoraggio dei social network

Il monitoraggio genererà un feed di informazioni risultante quale input del sistema di AI, elaborati internamente e deputati alla detection.
Gli alert generati in tale fase dovranno essere successivamente esaminati dall'operatore al fine di:
- evitare falsi positivi;
- fornire al Cliente le informazioni necessarie per procedere in proprio con azioni di take down ed alle eventuali denunce/querele.

Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Perimetro: domini e brand definiti in fase di contrattazione con il Cliente;
C. Modalità flat, senza limite al numero di segnalazioni;
D. Accessibilità ai dati: notifica via email, consultazione attraverso portale clienti e/o attraverso API;
E. Copertura temporale: h24 e 7/7 gg;
F. Periodo di erogazione: 36 mesi;
G. Azioni di contrasto non previste.

BRAND MONITOR
Monitoraggio delle diverse tecniche di typosquatting applicate ai domini istituzionali.
L'attività di Brand Monitor è deputata all'identificazione di domini di nuova registrazione aventi nomi sospetti e similari ai brand/domini del Cliente.
Il monitoraggio consta delle seguenti fasi:
- Detection automatizzata: attraverso servizi di appoggio e funzionalità sviluppate in proprio, per eseguire l'analisi di liste di nuovi domini al fine di identificare quelli con nomi palesemente simili al brand del Cliente. I servizi in uso dovranno permettere il monitoraggio dei più diffusi TLD dati con un ritardo di uno o due giorni, dipendentemente dalle tempistiche di diffusione degli stessi dai NIC di competenza o dalla distribuzione gerarchica dei DNS.
- Analisi svolta dall'operatore finalizzata ad escludere falsi positivi e a valutare la natura del dominio sospetto e del possibile impiego malevolo;

- Comunicazione: il dominio rilevato viene tempestivamente comunicato al Cliente affinché possa essere:
  - inserito nelle block list dei sistemi periferici al fine di bloccare email fraudolente dagli stessi inviate a danno della struttura aziendale;
  - Valutate possibili azioni di contrasto quali richieste take down, dispute dominio, ecc.
- Verifica periodica: in caso i domini non presentino grafica, loghi, marchi del Cliente gli stessi vengono mantenuti in monitoraggio e verificati ogni 6 ore.

Il servizio in oggetto risulta quindi idoneo a tutelare le aziende dalle azioni di phishing mirato, nelle quali i criminali fingendosi soggetti facente parte dell'organico aziendale scrivono a personale della società target facendo uso di indirizzi di posta elettronica con domini similari a quello del target al fine di richiedere l'emissione di pagamenti o inoculare software malevoli.
In un'ottica di difesa preventiva i domini individuati e ritenuti sospetti possono quindi essere inseriti nelle black list di firewall ed anti-spam affinché le mail fraudolente provenienti da essi non raggiungano mai il personale dell'organizzazione.

Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Perimetro: domini e brand definiti in fase in contrattazione con il Cliente;
C. Modalità flat, senza limite al numero di segnalazioni;
D. Accessibilità ai dati: notifica via email, consultazione attraverso portale clienti;
E. Copertura temporale: h24 e 7/7 gg;
F. Periodo di erogazione: 36 mesi;
G. Azioni di contrasto non previste.

DATA LEAK MONITOR
Segnalazione utenze / account mail compromesse relativamente dipendenti del Cliente.
L'attività è realizzata attraverso i servizi:

- Data Leak Monitor: deputato al monitoraggio degli ambienti underground al fine di rilevare il rilascio di dati estrapolati da siti web di qualsiasi dimensione in cui i dipendenti si siano registrati con l'indirizzo email aziendale, con il rischio di riutilizzo sui sistemi aziendali della medesima password;
- Recupero Email da Phishing: deputato a recuperare gli indirizzi email di coloro che cadono vittime di phishing a danno di qualsiasi tipologia di ente.

L'attività è tuttavia limitata all'acquisizione dei contenuti liberamente scaricabili. Il personale dell'Operatore Economico non dovrà opere l'acquisto di informazioni/dati messi in vendita in quanto:

- Eticamente discutibile, in quanto si favorisce il proliferare della attività criminali;
- Si configura il reato di ricettazione Art 648 C.P.;
- Tali spese non sono deducibili dalle imposte e necessiterebbero di fondi ad hoc non permessi dalla normativa vigente

Il servizio non si basa sulla consultazione limitata di servizi di terze parti, quali: Have I Been Pwned, How Safe Is Your Password? | BreachAlarm, etc, ma sull'effettiva ricerca, acquisizione ed analisi dei dati originali costituenti il dump.
Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Perimetro: domini e brand definiti in fase in contrattazione con il Cliente;
C. Modalità flat, senza limite al numero di segnalazioni;
D. Accessibilità ai dati: notifica via email, consultazione attraverso portale clienti, report pdf via email garantendo la confidenzialità delle informazioni;
E. Copertura temporale: h24 e 7/7 gg;

F. Periodo di erogazione: 36 mesi;

CTI MAIN CORE

L'attività di monitoraggio dei contenuti presenti sul Web nei sui diversi livelli di profondità, emerso, Deep e Dark, è svolta:

- attraverso il monitoraggio automatizzato delle piattaforme accessibili sul web emerso, attraverso connettori sviluppati ad hoc per collegare le sorgenti di informazioni alla Threat Intelligence Platform;
- la frequentazione dagli ambienti underground/cyber criminali, identificabili in Deep e Dark web, da parte dell'operatore facendo uso di profili ad hoc (sock puppets) credibili.

A seguito degli alert generati dalla TIP o dalla frequentazione in prima persona degli ambiti underground, il team di analisti esaminerà l'evidenza per determinare la sussistenza di una effettiva minaccia, nel qual caso sarà elaborato un report per il Cliente ed in caso di minaccia imminente o di elevata rilevanza si avrà un'immediata comunicazione di allerta verso il team sicurezza del committente.
Il servizio prevede inoltre l'erogazione di un report settimanale finalizzato a fornire una più completa informazione riguardo a notizie che hanno meritato l'attenzione di media generalisti e pubblicazioni del settore IT pubblica settimanalmente un approfondimento di Cyber Threat Intelligence che, in formato narrativo/discorsivo e con l'ausilio di grafici, riepiloga ogni inizio settimana gli eventi della settimana precedente.

Il report racconta complessivamente ciò che il team di analisti ha individuato e analizzato la settimana precedente, come le principali campagne di phishing, le principali campagne malware, i principali data leak e aziende compromesse da attacchi ransomware o che hanno subito attacchi DDoS ma altresì narra anche di eventi nazionali e internazionali attinenti alla Cyber Threat Intelligence.
Infine riepiloga i CVE maggiormente impattanti recentemente identificati.

Il servizio risponde alle caratteristiche nel seguito elencate:
A. Svolto secondo le modalità sopra descritte;
B. Copertura temporale: h24 e 7/7 gg;
C. Periodo di erogazione: 36 mesi;
D. Perimetro: domini e brand definiti in fase in contrattazione con il Cliente;
E. Si richiede scambio informativo relativo ad antagonisti o elementi avversi già noti;
F. Accessibilità ai dati: consultazione attraverso portale clienti, report pdf via email garantendo la confidenzialità delle informazioni;
G. Le evidenze sono notificate al Cliente via report in formato pdf:

- Report di livello "non classificato" sono:
  - inviati via email senza protezione alcuna
  - resi disponibili attraverso il portale clienti dedicato
- Report di livello "confidenziale", "riservato" e "segreto" sono inviati via:
  - file protetto da password (pdf/zip/rar);
  - resi disponibili attraverso il portale clienti dedicato.

IOC ZONE - CONDIVISIONE INDICATORI DI COMPROMISSIONE

Il servizio è finalizzato alla condivisione di indicatori di compromissione (IoC) derivanti dall'analisi statica ed in sandbox dei malware per sistemi desktop e mobili, identificati attraverso la raccolta su apposite spamtrap gestite dall'operatore attraverso i monitoraggi web svolti con automatismi e ricerche.

Le analisi condotte consentono di estrapolare e condividere verso il Cliente tutte quelle informazioni utili a:

- Evitare che le mail spam possano essere ricevute dai dipendenti;
- Bloccare connessioni pericolose verso ulteriori malware e server C&C;

- Identificare attraverso sistemi SIEM device già compromessi presenti nelle reti interne.

La condivisione dei dati può avvenire attraverso le specifiche metodiche e strutture usualmente impiegate per tale tipologia di servizi, quali istanza MISP o formato Stix via protocollo Taxi, o con metodiche e formati specificamente customizzati per il Cliente.

A. Svolto secondo le modalità sopra descritte;
B. Modalità flat, senza limite al numero di segnalazioni;
C. Accessibilità ai dati: attraverso la metodica ed il formato concordato con il Cliente;
D. Copertura temporale: h24 7/7 gg;
E. Periodo di erogazione: 36 mesi;

COMUNICAZIONI E REPORT

Le attività sopra descritte genereranno comunicazioni secondo le modalità sotto indicate

Monitoraggio	Notifica via email	Report PDF	Dati accessibili a portale	API/Misp/ecc.
Anti-phishing	X		X	X
Brand Monitor	X		X	
Data Leak Monitor		X	X	
CTI Main Core		X	X	
IoC Zone				X

COPERTURA TEMPORALE E SLA

I monitoraggi di Cyber Threat Intelligence descritti nel presente documento sono continui 24h/24, 365gg/ 365.
L'Operatore dovrà garantire la presa in carico e gestione delle richieste inoltrate dal Cliente:

- Nei giorni feriali: entro 6 (sei) ore dalla data/ora di inoltro richiesta da parte di personale del Cliente;
- Nei giorni festivi: entro 12 (dodici) ore di inoltro richiesta da parte di personale del Cliente.