Allegato 8

MODELLO DI DICHIARAZIONE DI COMPLIANCE DI CYBERSICUREZZA E DI IMPEGNO CONTRATTUALE IN MATERIA DI SICUREZZA INFORMATICA, CATENA DI APPROVVIGIONAMENTO E PROTEZIONE DEI SISTEMI INFORMATIVI

RILASCIATO ANCHE AI SENSI DEGLI ARTT. 46 E 47 DEL D.P.R. 445/2000
(Non è ammessa la sostituzione dei certificati e delle dichiarazioni con fotocopie e duplicati non autenticati nelle forme previste dagli articoli 18 e 19 del D.P.R. n. 445/2000)

Spett.le
REGIONE PUGLIA
Sezione Cloud, Cybersecurity e Infrastrutture Tecnologiche
Lungomare Nazario Sauro, 33
70121 Bari

OGGETTO: DICHIARAZIONE AI SENSI DEL D.P.R. 445/2000 RELATIVA ALLA COMPLIANCE NORMATIVA IN MATERIA DI CYBERSICUREZZA PER LA PROCEDURA/AFFIDAMENTO:

Procedura ristretta, ai sensi dell'art. 72 del D. Lgs. n. 36/2023, da svolgersi mediante il Sistema Dinamico di Acquisizione per la Pubblica Amministrazione (SDAPA), da aggiudicare con il criterio del minor prezzo, per l'affidamento della fornitura di licenze Alfresco Enterprise e dei relativi servizi di manutenzione e assistenza per la durata di mesi 36 in favore della Regione Puglia

Il/La sottoscritto/a _____, nato/a a _____ il _____, C.F. _____, domiciliato per la carica presso la sede societaria ove appresso, nella sua qualità di _____ e legale rappresentante avente i poteri necessari per impegnare la _____ nella presente procedura, con sede in _____, Via _____ n. ___, Città _____, Provincia ___, Paese _____, iscritta al Registro delle Imprese di _____ al n. _____, codice fiscale/P. IVA n. _____, di seguito denominato "operatore economico",

ai sensi degli artt. 46 e 47 del D.P.R. 28/12/2000, n. 445, consapevole del fatto che, in caso di dichiarazione mendace, saranno applicate nei suoi riguardi, ai sensi dell'art. 76 dello stesso decreto, le sanzioni previste dal codice penale e dalle leggi speciali in materia di falsità negli atti e dichiarazioni mendaci, oltre alle conseguenze amministrative previste per le procedure concernenti gli appalti pubblici,

SCHEDA DI INQUADRAMENTO DELL'AFFIDAMENTO

La presente dichiarazione è resa con riferimento alla procedura/affidamento sopra indicata, avente ad oggetto:
☐ fornitura di prodotti hardware o appliance di sicurezza
☐ fornitura di software, licenze o piattaforme ICT/cyber
☐ servizi di manutenzione, assistenza o supporto specialistico
☐ servizi cloud, SaaS, PaaS, IaaS o infrastrutture digitali
☐ servizi gestiti di cybersicurezza, monitoraggio, SOC, SIEM, EDR/XDR, vulnerability management o analoghi
☐ servizi che comportano accesso, anche remoto, a sistemi, reti, dati, log, configurazioni o ambienti della Regione Puglia
☐ altro: _____

L'operatore economico prende atto che le dichiarazioni e gli impegni di seguito riportati trovano applicazione secondo un approccio basato sul rischio e sono commisurati alla natura, all'oggetto e alla criticità dell'affidamento, tenendo conto dell'eventuale trattamento di dati personali, dell'accesso a sistemi, reti, ambienti cloud, log, configurazioni o

infrastrutture della Regione Puglia, nonché dell'applicabilità della normativa nazionale ed europea in materia di cybersicurezza.

DICHIARA SOTTO LA PROPRIA RESPONSABILITÀ E SI IMPEGNA, PER QUANTO DI COMPETENZA, A GARANTIRE QUANTO SEGUE

a) Conformità normativa e proporzionalità delle misure.

L'operatore economico dichiara di adottare misure tecniche, organizzative e operative idonee a garantire la cybersicurezza dei beni, servizi, tecnologie, manutenzioni e/o apparecchiature oggetto dell'affidamento, secondo criteri di adeguatezza, proporzionalità e gestione del rischio, tenendo conto della natura, delle caratteristiche e della criticità della fornitura, nonché del potenziale impatto sui sistemi, sulle reti, sui servizi digitali e sulle informazioni della Regione Puglia.

A tal fine, l'operatore economico dichiara di effettuare, ove applicabile in relazione all'oggetto dell'affidamento, attività di identificazione, analisi, valutazione e trattamento dei rischi di cybersicurezza connessi ai prodotti, servizi, sistemi e infrastrutture utilizzati per l'esecuzione delle prestazioni contrattuali, adottando misure di prevenzione, protezione, rilevazione, risposta e recupero proporzionate ai rischi individuati e mantenendo adeguate evidenze documentali delle valutazioni effettuate e delle misure adottate.

L'operatore economico dichiara altresì di tenere conto, ove applicabili in relazione all'oggetto dell'affidamento, delle disposizioni di cui alla Legge 28 giugno 2024, n. 90, al Decreto Legislativo 4 settembre 2024, n. 138, al DPCM 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025, al Decreto Direttoriale ACN n. 21007/2024, nonché delle ulteriori determinazioni, linee guida, raccomandazioni, misure attuative e indicazioni emanate dall'Agenzia per la Cybersicurezza Nazionale e dalle altre Autorità competenti in materia di cybersicurezza applicabili alla specifica fornitura.

b) Origine delle tecnologie, supply chain e componentistica.

Ove applicabile, l'operatore economico dichiara che i componenti hardware, software, firmware, servizi, piattaforme, infrastrutture cloud, appliance, apparati, licenze e tecnologie impiegate per l'esecuzione della fornitura sono originarie dell'Italia, o di Paesi dell'Unione Europea, o di Paesi aderenti all'Alleanza atlantica (NATO), o di Paesi terzi di cui all'Allegato 3 del DPCM del 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025.

Ove richiesto dalla Stazione appaltante, l'operatore economico si impegna a fornire documentazione utile alla verifica della catena di fornitura, inclusa, se pertinente, Bill of Materials, Software Bill of Materials, elenco dei componenti software di terze parti, produttori, subfornitori, versioni e dipendenze principali.

L'operatore economico si impegna a comunicare tempestivamente eventuali variazioni rilevanti della catena di fornitura, dei produttori, dei subfornitori, dei cloud provider, dei managed service provider o dei componenti tecnologici utilizzati nell'esecuzione dell'affidamento.

c) Governance e sicurezza organizzativa.

L'operatore economico dichiara di disporre, in relazione alla natura e alla criticità dell'affidamento, di misure documentate di governance della sicurezza delle informazioni, comprendenti, ove applicabile: ruoli e responsabilità interne, politiche di sicurezza, gestione del rischio cyber, formazione del personale, gestione degli accessi, gestione delle vulnerabilità, incident response, continuità operativa e controllo dei fornitori o subfornitori coinvolti.

d) Misure tecniche di protezione.

Ove applicabile, l'operatore economico dichiara che i sistemi, i servizi e le tecnologie utilizzati per l'esecuzione della fornitura garantiscono misure coerenti con lo stato dell'arte, tra cui:

– inventario aggiornato degli asset hardware e software rilevanti;
– gestione delle vulnerabilità e tempestiva applicazione delle patch di sicurezza;
– gestione degli accessi secondo i principi di necessità, minimo privilegio e tracciabilità;
– utilizzo di utenze nominative e divieto di credenziali condivise, salvo casi eccezionali autorizzati e tracciati;
– autenticazione forte per accessi remoti, amministrativi o privilegiati, ove tecnicamente possibile;
– configurazioni sicure, hardening e disabilitazione di servizi, porte, account o protocolli non necessari;
– cifratura e protezione dei dati, delle credenziali e delle configurazioni, ove pertinente;

– raccolta, protezione e conservazione dei log secondo quanto previsto dal contratto, dalle policy della Regione Puglia o dalla normativa applicabile;
– sistemi anti-malware, ove pertinenti, e misure di backup e ripristino periodicamente verificate;
– supporto, manutenzione e aggiornamenti di sicurezza per l'intera durata contrattuale e secondo la normativa vigente, salvo diversa indicazione espressa nella documentazione dell'affidamento.

L'operatore economico si impegna a comunicare alla Regione Puglia eventuali vulnerabilità critiche o elevate che interessino i beni o servizi forniti, indicando impatto, componenti interessati, misure di mitigazione e tempi di rilascio o applicazione degli aggiornamenti.

e) Perimetro di Sicurezza Nazionale Cibernetica, Legge 90/2024 e DPCM 30 aprile 2025.

Ove l'affidamento riguardi beni, sistemi o servizi ICT destinati a essere impiegati in contesti soggetti alla disciplina del Perimetro di Sicurezza Nazionale Cibernetica o comunque connessi alla tutela degli interessi nazionali strategici e della sicurezza nazionale, l'operatore economico si impegna a fornire alla Stazione appaltante il supporto tecnico-documentale necessario alle verifiche previste dalla normativa applicabile.

A tal fine, l'operatore economico si impegna a rendere disponibili, ove richiesti, informazioni relative a componenti hardware, software, firmware, configurazioni, vulnerabilità note, misure di mitigazione, produttori, subfornitori, infrastrutture cloud, servizi gestiti, modalità di aggiornamento e documentazione tecnica.

Gli eventuali oneri derivanti da verifiche, test, adeguamenti o attività aggiuntive saranno disciplinati dalla documentazione di gara, dal contratto, dall'ordine o dagli atti dell'affidamento.

f) Incident Response e Business Continuity.

L'operatore economico dichiara di disporre, ove applicabile, di procedure per la gestione degli incidenti informatici e di misure di continuità operativa coerenti con la natura dei servizi forniti.

L'operatore economico si impegna a comunicare alla Regione Puglia, senza ingiustificato ritardo e secondo le modalità previste dalla documentazione contrattuale, ogni incidente, sospetto incidente, vulnerabilità critica, accesso non autorizzato, perdita di disponibilità, integrità o riservatezza, data breach o altro evento di sicurezza che possa incidere sui beni, servizi, sistemi, dati, log, configurazioni o infrastrutture oggetto dell'affidamento.

La comunicazione dovrà contenere, ove disponibili: descrizione dell'evento, data e ora di rilevazione, sistemi o servizi interessati, impatto stimato, misure adottate, azioni di mitigazione e referente tecnico per la gestione dell'evento.

L'operatore economico si impegna a collaborare con la Regione Puglia per consentire l'eventuale adempimento degli obblighi di notifica verso le autorità competenti.

g) Disponibilità ad audit, verifiche e assessment.

L'operatore economico si impegna a rendere disponibili, su richiesta della Stazione appaltante e con congruo preavviso, le evidenze documentali, organizzative e tecniche necessarie a verificare il rispetto degli obblighi di cybersicurezza relativi alla fornitura.

Le verifiche potranno consistere, in ragione della criticità dell'affidamento, in audit documentali, questionari di sicurezza, assessment tecnici, verifica di certificazioni, report di vulnerability assessment o penetration test, evidenze di backup test, piani di continuità operativa, policy di sicurezza, elenco dei subfornitori, BOM/SBOM, documentazione di patch management e report di remediation.

Eventuali non conformità dovranno essere gestite mediante piano di rientro, con indicazione delle misure correttive, dei tempi di attuazione e delle evidenze di chiusura.

h) Subappaltatori, subfornitori, terze parti e personale.

Su richiesta della stazione appaltante l'operatore economico si impegna a fornire un elenco dei subappaltatori, subfornitori, produttori, partner tecnologici, cloud provider, managed service provider o ulteriori soggetti terzi coinvolti nell'esecuzione della fornitura o aventi accesso a dati, sistemi, configurazioni, log, ambienti, infrastrutture o informazioni della Regione Puglia.

Inoltre, in caso di forniture aventi ad oggetto servizi di cybersicurezza, l'operatore economico si impegna a comunicare elenco del personale con dettaglio dei ruoli e responsabilità.

Ogni variazione rilevante dei soggetti terzi coinvolti dovrà essere comunicata alla Stazione appaltante.

L'operatore economico resta responsabile dell'operato dei soggetti terzi coinvolti e garantisce il ribaltamento degli obblighi di cybersicurezza, riservatezza, protezione dei dati, gestione degli incidenti e collaborazione agli audit lungo la catena di fornitura.

i) Servizi cloud, infrastrutture digitali e localizzazione dei dati.

Ove la fornitura preveda l'utilizzo di servizi cloud, infrastrutture digitali, piattaforme SaaS/PaaS/IaaS o servizi erogati tramite ambienti cloud, l'operatore economico dichiara il servizio cloud impiegato, il provider, la localizzazione geografica dei dati, il livello di qualificazione ACN ove applicabile, le misure di cifratura, backup, logging, continuità operativa, portabilità ed exit strategy, nonché l'elenco degli eventuali subfornitori o sub-responsabili coinvolti.

L'operatore economico si impegna a non trasferire dati, log, configurazioni, credenziali o informazioni della Regione Puglia verso ambienti, regioni geografiche, cloud provider o subfornitori diversi da quelli dichiarati, salvo preventiva comunicazione alla Stazione appaltante e relativa autorizzazione, ove necessaria.

j) Protezione dei dati personali e riservatezza.

Ove l'esecuzione dell'affidamento comporti trattamento di dati personali per conto della Regione Puglia, l'operatore economico prende atto che la presente dichiarazione non sostituisce l'eventuale atto di designazione a Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679, né gli ulteriori adempimenti previsti dalla normativa vigente.

L'operatore economico si impegna a mantenere riservate le informazioni, configurazioni, credenziali, architetture, documentazione tecnica, log, vulnerabilità, incidenti, misure di sicurezza e ogni altra informazione appresa nell'ambito dell'affidamento.

k) Obblighi essenziali, rimedi contrattuali e veridicità delle dichiarazioni.

Le dichiarazioni e gli impegni contenuti nel presente modello costituiscono, ove richiamati nella documentazione di gara, nell'ordine, nel contratto o negli atti dell'affidamento, obblighi rilevanti ai fini della corretta esecuzione della fornitura.

La mancata veridicità delle dichiarazioni, l'omessa comunicazione di incidenti o vulnerabilità rilevanti, la mancata collaborazione agli audit, la sostituzione non comunicata di subfornitori critici, la mancata adozione delle misure correttive richieste o la violazione degli obblighi di riservatezza e sicurezza potranno comportare, secondo la gravità del caso e nel rispetto della normativa sui contratti pubblici, l'applicazione dei rimedi previsti dal contratto, incluse contestazioni di inadempimento, penali, sospensione delle attività, risoluzione o ulteriori conseguenze previste dalla legge e dalla documentazione contrattuale.

_____, lì _____

Firma

_____
(firmato digitalmente)