si di iscrizioni e pendenze pro capite sensibilmente inferiori alle medie nazionali, e di un posto di sostituto procuratore ciascuna le piante organiche delle procure della Repubblica presso i tribunali di Santa Maria Capua Vetere e Benevento, per cui si rilevano analoghe condizioni per flussi di lavoro e numero di posti vacanti;

Valutato che, in coerenza con i criteri generali adottati, le due unità necessarie al rafforzamento mirato della procura della Repubblica presso il tribunale di Ivrea possono essere reperite riducendo di una unità ciascuna le piante organiche delle procure della Repubblica presso i tribunali di Alessandria e Torino, che presentano posti vacanti non pubblicati e indici favorevoli quanto alle iscrizioni pro capite;

Acquisito al riguardo il parere del Consiglio superiore della magistratura che, nella seduta del 15 novembre 2023, ha ritenuto, con separate delibere, di esprimere parere favorevole alle modifiche di organico proposte, condividendo le motivazioni a sostegno dell'intervento, la consistenza numerica degli incrementi e le scelte operate per l'individuazione delle unità necessarie;

Decreta

Art. 1

Le piante organiche del personale di magistratura del tribunale di Napoli Nord e delle procure della Repubblica presso i tribunali di Napoli Nord e Ivrea sono ampliate, rispettivamente, di dieci posti di giudice, di tre posti di sostituto procuratore e di due posti di sostituto procuratore.

Art. 2

La dotazione nazionale delle piante organiche flessibili distrettuali di magistrati, da destinare alla sostituzione dei magistrati assenti ovvero all'assegnazione agli uffici giudiziari del distretto che versino in condizioni critiche di rendimento, è fissata in 176 unità, di cui 123 con funzioni giudicanti e 53 con funzioni requirenti, così modificando il decreto ministeriale 23 marzo 2022.

La pianta organica flessibile distrettuale di magistrati del distretto di Napoli è ridotta di due unità destinate alle funzioni giudicanti e di una unità destinata alle funzioni requirenti.

Art. 3

La pianta organica del personale di magistratura del tribunale di Napoli è ridotta di tre posti di giudice e quelle delle procure della Repubblica presso i tribunali di Alessandria, Benevento, Santa Maria Capua Vetere e Torino sono ridotte di un posto di sostituto procuratore ciascuna.

Art. 4

Le tabelle B ed E vigenti allegate al decreto ministeriale 14 settembre 2020, registrato alla Corte dei Conti il 7 ottobre 2020, sono modificate nel senso e nei limiti di quanto previsto dagli articoli che precedono.

Roma, 22 novembre 2023

Il Ministro
CARLO NORDIO

Decreto Ministeriale 5 gennaio 2024 – Requisiti tecnici specifici per la gestione dei dati presso le infrastrutture digitali interdistrettuali, ai sensi dell'articolo 2, comma2, del decreto legge 10 agosto 2023, n. 105

Visto il decreto del Presidente della Repubblica 22 settembre 1988, n. 447, recante approvazione del codice di procedura penale;

Visto il decreto legislativo 28 luglio 1989, n. 271, recante norme di attuazione, di coordinamento e transitorie del codice di procedura penale;

Vista la legge 23 giugno 2017, n. 103, recante modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario;

Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017 – e, in particolare, l'articolo 11 relativo all'attuazione della direttiva (UE) 2016/680;

Visto il decreto legislativo 29 dicembre 2017, n. 216, recante disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103;

Visto l'articolo 2, comma 2, del decreto del Ministro della Giustizia 20 aprile 2018, recante disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'articolo 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216;

Visto il decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione;

Visto il decreto del Ministro della Giustizia 6 ottobre 2023, adottato ai sensi dell'articolo 2, comma 2, del decreto-legge 10 agosto 2023, n. 105;

Visto il decreto legislativo del 7 marzo 2005 n. 82 e successive modificazioni, recante Codice dell'amministrazione digitale (CAD) e successive modifiche;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali e successive modifiche;

Vista la direttiva (UE) 2022/2555 del parlamento europeo e del consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (c.d. direttiva NIS 2);

Visto il decreto legislativo 18 maggio 2018, n. 51 recante attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

Visto il decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

Sentiti il Consiglio superiore della magistratura, il Garante per la protezione dei dati personali e il Comitato interministeriale per la cybersicurezza;

Decreta

Articolo 1
Definizioni

1. Agli effetti del presente decreto si intende per:

a) «autenticità»: capacità di identificare con certezza la provenienza di dati e informazioni, ossia verificare l'identità dell'origine;

b) «integrità»: caratteristica relativa alla necessità per dati e informazioni memorizzate in un sistema o scambiate tra due entità di essere protette da modifiche non autorizzate;

c) «riservatezza»: accessibilità a dati e informazioni solo da parte di utenti e processi che ne hanno diritto, in base alle policy definite nel sistema;

d) «disponibilità»: la probabilità che un sistema, un'apparecchiatura o un impianto, siano in grado di funzionare in un dato momento, indipendentemente dai guasti e dalle riparazioni intervenuti fino allora, e rimanga operativo in circostanze normali per servire allo scopo previsto;

e) «sistema di ripristino»: insieme di apparati tecnologici, meccanismi e processi che consentono, in conseguenza di eventi disastrosi e ove possibile stanti i limiti tecnologici del sistema stesso, il recupero dei dati e delle informazioni memorizzate e la continuità operativa di una piattaforma tecnologica;

f) «conferimento»: processo di riversamento dei verbali e delle registrazioni trasmesse al pubblico ministero dalla polizia giudiziaria nell'archivio digitale di cui all'articolo 269, comma 1, del codice di procedura penale;

g) «evento»: porzione del conferimento corrispondente al minimo contenuto per il quale può essere concessa l'autorizzazione alla fruizione, anche eventualmente per suoi sotto intervalli temporali, ove previsto;

h) «retrocompatibilità»: caratteristica di una versione di un software che consente di aprire correttamente tutti i dati salvati utilizzando versioni precedenti;

i) «trasferimento logico»: trasferimento di un dato che non ne implica lo spostamento fisico, ottenuto attraverso una modifica delle regole di visibilità associate ad esso;

j) «hash crittografico»: funzione deterministica e non invertibile che mappa un dato arbitrario in input in una stringa di lunghezza predefinita;

k) «meccanismo di autenticazione del dato»: processo che consente di associare ad un dato il relativo hash crittografico, generato anche utilizzando in ingresso alla funzione di hash uno o più segreti di natura simmetrica;

l) «firma digitale»: firma elettronica, ossia insieme di dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici utilizzati come metodo di identificazione informatica, basata su un certificato qualificato ovvero su un sistema di chiavi crittografiche, e realizzata mediante un dispositivo sicuro, così come disciplinato dall'articolo 24 del decreto legislativo del 7 marzo 2005 n. 82;

m) «crittografia»: metodo di codifica e protezione dei dati, definito per impedire ad estranei di accedere alle informazioni senza essere dotati di autorizzazione;

n) «chiave»: stringa utilizzata come parametro di input di un algoritmo crittografico;

o) «chiavi asimmetriche»: la coppia di chiavi, una pubblica ed una privata, correlate tra loro e utilizzate, con funzione reciproca, in input a meccanismi di crittografia asimmetrica;

p) «chiave privata»: chiave asimmetrica facente parte di una coppia di chiavi e legata univocamente alla corrispondente chiave pubblica; viene utilizzata solo dal proprietario della coppia di chiavi, in quanto è nota soltanto al proprietario stesso;

q) «chiave pubblica»: chiave asimmetrica facente parte di una coppia di chiavi e legata univocamente alla corrispondente chiave privata; pur essendo di proprietà di uno specifico soggetto, per sua natura questa chiave deve essere resa pubblica al fine di utilizzare meccanismi di crittografia asimmetrica;

r) «chiave simmetrica»: chiave utilizzata in input ad un algoritmo di tipo simmetrico condivisa tra tutti gli utenti autorizzati ad eseguire l'algoritmo sul dato trattato;

s) «file contenitore»: singolo file contenente un insieme di altri file;

t) «attacco brute force»: in crittografia, metodo che si utilizza per trovare la chiave di un sistema, provando tutte le possibili combinazioni o, per estensione, attraverso l'utilizzo di un dizionario;

u) «Identity Access Management (IAM)»: sistema integrato di tecnologie, regole e processi per controllare gli accessi degli utenti ad applicazioni e dati;

v) «Active Directory (AD)»: sistema commerciale che consente di catalogare, raggruppandoli secondo la struttura organizzativa, risorse, servizi e utenti all'interno di "domini" e di gestire l'autenticazione degli utenti;

w) «single sign-on (SSO)»: sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato;

x) «gateway»: unico punto in cui confluiscono reti e/o dati e/o comunicazioni provenienti da molteplici sorgenti differenti;

y) «provider»: nei sistemi di autenticazione, entità che attestano l'identità dei soggetti che eseguono il processo di autenticazione;

z) «OpenID Connect»: standard di autenticazione utilizzato nelle applicazioni web e mobile, caratterizzato da alti livelli di flessibilità e sicurezza, semplicità di implementazione ed efficacia nell'interoperabilità;

aa) «OAuth2.0»: protocollo standard aperto che consente alle applicazioni di accedere alle risorse protette di un servizio per conto dell'utente;

bb) «firewall»: dispositivo di sicurezza di rete, composto da hardware e/o software, che filtra il traffico di rete in ingresso e in uscita e autorizza o blocca i pacchetti di dati in base a specifiche regole di sicurezza, creando una barriera che evita comunicazioni non autorizzate, proteggendo di fatto i dispositivi connessi da potenziali attacchi informatici;

cc) «Public Key Infrastructure (PKI)»: l'architettura, l'organizzazione, le tecniche, le pratiche e le procedure che complessivamente supportano l'implementazione e l'operatività di un sistema crittografico basato su chiave pubblica, unitamente a un processo per l'emissione, il mantenimento e la revoca di certificati a chiave pubblica;

dd) «Privileged Access Management (PAM)»: una soluzione per la sicurezza delle identità che contribuisce a proteggere le organizzazioni contro minacce cibernetiche attraverso il monitoraggio, l'identificazione e la prevenzione di accessi non autorizzati a risorse critiche;

ee) «Virtual Private Network (VPN)»: ambiente comunicativo in cui l'accesso alle risorse della rete è controllato in modo da permettere la comunicazione tramite connessioni paritarie solo all'interno di una ben definita comunità di interesse nonostante tali connessioni possano essere realizzate utilizzando un'infrastruttura di rete pubblica e condivisa, quale ad esempio internet.

ff) «misure tecnico-organizzative»: documento che contiene le disposizioni che assicurano il corretto funzionamento delle infrastrutture digitali interdistrettuali;

Articolo 2
Oggetto e ambito di applicazione

1. Ferma restando l'applicazione delle misure di sicurezza di cui al regolamento adottato con decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, con il presente decreto sono definiti i requisiti tecnici specifici che assicurano l'autenticità, l'integrità, la riservatezza e la disponibilità dei dati gestiti dai sistemi informativi funzionali alle attività di intercettazione eseguite da ciascun ufficio del pubblico ministero, anche in relazione al conferimento e ai sistemi di ripristino. È inoltre disciplinato il collegamento telematico tra le infrastrutture digitali interdistrettuali istituite con il decreto ministeriale 6 ottobre 2023 e gli impianti installati nella procura della Repubblica, garantendo il massimo livello di sicurezza e riservatezza.

2. Le infrastrutture digitali interdistrettuali rese disponibili dal Ministero assicurano la memorizzazione e conservazione delle conversazioni e delle comunicazioni intercettate nell'ambito di un procedimento penale e ricevute sugli impianti installati nella procura della Repubblica. Le infrastrutture digitali interdistrettuali saranno inoltre attrezzate per le operazioni di intercettazione secondo l'evoluzione tecnologica.

3. Le infrastrutture digitali interdistrettuali assicurano altresì che le attività di intercettazione relative a procedimenti iscritti successivamente al 28 febbraio 2025 siano eseguite, in quanto compatibili e salvo diversa ulteriore espressa disposizione, nel rispetto dei requisiti tecnici e funzionali determinati dagli articoli 2, 3 e 4 del decreto interministeriale del 6 ottobre 2022.

4. I sistemi di ripristino di cui al comma 1 del presente articolo sono nativamente integrati all'interno della piattaforma tecnologica di memorizzazione dei dati operativa presso le infrastrutture digitali interdistrettuali del Ministero. Tali sistemi assicurano la piena funzionalità della piattaforma tecnologica di memorizzazione dei dati anche in caso di totale indisponibilità di una delle infrastrutture digitali interdistrettuali in conseguenza di eventi disastrosi.

5. Le infrastrutture digitali interdistrettuali e i sistemi di cui al presente decreto si conformano ai seguenti requisiti tecnici:

a. il processo di conferimento deve consentire il trasferimento dei file relativi agli eventi costituenti l'intercettazione, ivi compresi i metadati associati ad essi e, in ogni caso, tutti i dati necessari per garantire la corretta fruizione dei contenuti;

b. il processo di consultazione deve consentire l'accesso, previa autorizzazione qualora prevista e necessaria, in sola lettura a eventi, o a parti di essi, da parte dei soggetti di cui all'articolo 89-bis, comma 3, del decreto legislativo 28 luglio 1989, n. 271;

c. nei casi di trasferimento per competenza dei procedimenti penali verso ufficio giudiziario diverso da quello che ha disposto ed eseguito le intercettazioni, tale trasferimento deve consentire il contestuale trasferimento logico dei file relativi agli eventi costituenti l'intercettazione al fine di consentirne l'utilizzo ai soggetti destinatari, garantendo l'autenticità, l'integrità e la riservatezza dei contenuti;

d. in caso di trasmissione ad altro ufficio giudiziario di contenuti ritenuti di interesse per altre indagini ovvero di consegna a terze parti autorizzate di copia delle intercettazioni, deve essere realizzato un processo di estrazione di eventuali copie dalla piattaforma tecnologica di memorizzazione dei dati operativa presso le infrastrutture digitali interdistrettuali, che consenta l'esportazione di tutti e soli i contenuti e/o porzioni di essi autorizzati, garantendo l'autenticità, l'integrità e la riservatezza dei contenuti oltre che l'autenticazione del soggetto destinatario;

e. i sistemi devono essere realizzati in modo da garantire la gestione sia degli eventi e dati costituenti nuove intercettazioni sia di quelli già presenti in archivio al momento dell'entrata in vigore del presente decreto;

f. nel caso in cui siano mantenuti in archivio eventi e dati di intercettazioni conferiti nei formati gestiti prima dell'entrata in vigore del presente decreto i software necessari per la visualizzazione ed il trattamento dei contenuti – di tutte le versioni disponibili e tale da rendere possibile la consultazione di tutti i file storicamente conferiti – devono essere conservati in un repository dedicato;

g. il processo di consultazione deve garantire la retrocompatibilità con tutti i formati di file costituenti le intercettazioni in uso da parte delle procure;

h. i requisiti tecnici delle infrastrutture digitali interdistrettuali devono garantire l'autonomia delle funzioni del procuratore della Repubblica di direzione, organizzazione e sorveglianza sulle attività di intercettazione e sul trattamento dei relativi dati, nonché sugli accessi e sulle operazioni compiute sui dati stessi, restando escluso, in ogni caso, l'accesso ai dati in chiaro da parte di soggetti non autorizzati dal procuratore della Repubblica.

i. i sistemi devono essere realizzati in modo tale da garantire i processi di consultazione dei dati da parte dei soggetti destinatari anche mediante idonei canali di collegamento tra le infrastrutture digitali interdistrettuali e gli impianti degli uffici di procura tali da supportare i trasferimenti di dati;

Articolo 3
Autenticità e integrità dei dati

1. Ai fini di assicurare l'autenticità e l'integrità dei dati di cui all'articolo 2 dal momento in cui viene effettuato il conferimento sino a quando i dati vengono utilizzati secondo quanto previsto dalla normativa, ciascun evento oggetto di conferimento deve essere processato mediante meccanismi di autenticazione del dato e/o di firma digitale.

2. I meccanismi adottati per assicurare l'integrità e l'autenticità dei dati garantiscono la capacità di rilevare eventuali alterazioni dei dati per cause accidentali o intenzionali, nonché il ripristino degli stessi.

3. Ogni intervento attuato dal Ministero sul sistemi che possa incidere sulla funzionalità dei sistemi stessi è preceduto da una interlocuzione con il procuratore della Repubblica. Sono assicurate in ogni caso la tracciabilità e la immediata e diretta conoscibilità da parte del procuratore della Repubblica di ogni accesso o intervento di manutenzione o di assistenza sulle infrastrutture e sui software, nonché di qualsiasi altra attività di accesso, acquisizione, trattamento e recupero dei dati.

Articolo 4
Riservatezza dei dati

1. Al fine di assicurare la riservatezza e la sicurezza dei dati di cui all'articolo 2, sono adottate idonee pratiche di sicurezza informatica, quali crittografia e restrizioni di accesso, sia fisiche sia digitali.

2. Tutti gli eventi costituenti le intercettazioni di cui all'articolo 2, comma 2, sono contenuti in un file contenitore criptato mediante un algoritmo simmetrico caratterizzato da idonea robustezza.

3. La chiave simmetrica utilizzata come input dell'algoritmo di cui al comma 2 del presente articolo deve essere trasmessa alla procura garantendone la segretezza attraverso un processo di ulteriore cifratura della stessa basato sull'impiego di chiavi asimmetriche assegnate alle Procure e gestite tramite una Public Key Infrastructure.

4. L'accesso ai dati delle intercettazioni è regolamentato attraverso politiche di gestione delle chiavi che limitano l'operazione di decriptazione dei contenuti esclusivamente ai soggetti preposti all'esecuzione del meccanismo di decifratura della chiave, ossia i soggetti che hanno facoltà di accedere ai dati senza ulteriori autorizzazioni da parte di soggetti terzi.

5. L'accesso ai dati è regolato da una piattaforma di Identity Access Management (IAM), che implementa le modalità di accesso previste dall'articolo 64 del decreto legislativo 7 marzo 2005, n. 82 e dal regolamento UE n. 910/2014 del 23 luglio 2014, in coordinamento con quanto previsto in materia di protezione dei dati personali, dalla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio e dal decreto legislativo 18 maggio 2018, n. 51.

6. La piattaforma di cui al comma 5 garantisce il controllo e la centralizzazione di identità, gruppi, policy e configurazioni. Per la gestione delle utenze può essere impiegato un sistema di autenticazione, eventualmente federato con l'Active Directory Nazionale, ferme restando le esigenze di segregazione delle utenze, per motivi di sicurezza. Inoltre, la piattaforma fornisce le informazioni dei gruppi e dei ruoli associati alle utenze riconosciute, permettendo la corretta gestione dei permessi. Tale gestione è assicurata sia per le utenze ordinarie che per le utenze esterne.

7. Il modello della piattaforma di cui al comma 5 è implementato in conformità con i seguenti principi architetturali:

a. utilizzo di autenticazione federata in single sign-on (SSO) tramite un gateway che renda trasparente l'aggiunta/rimozione/modifica dei provider;

b. utilizzo di standard di accesso sicuri, quali ad esempio OpenID Connect e OAuth2.0, con eventuale supporto di protocolli che garantiscano la retrocompatibilità;

c. utilizzo di sistemi di controllo di accesso ibridi basati su ruolo e su attributo e su policy;

d. governo del sistema mediante l'utilizzo di politiche centralizzate, gestite da una apposita struttura;

e. orientamento all'automazione e al monitoraggio, per abilitare la possibilità di prevenire – ove possibile – gli incidenti di sicurezza e di reagire tempestivamente con interventi mirati ed automatici.

f. autenticazione multifattore e assegnazione dei permessi secondo gli approcci just-in-time e just-enough in ottica zero trust.

8. Gli accessi amministrativi alla piattaforma sono gestiti tramite un sistema di Privileged Access Management.

Articolo 5

Collegamento telematico tra le infrastrutture istituite con il decreto ministeriale 6 ottobre 2023 e gli impianti installati nella procura della Repubblica

1. Il collegamento telematico tra le infrastrutture istituite con il decreto ministeriale 6 ottobre 2023 e gli impianti installati nella procura della Repubblica è instaurato attraverso l'utilizzo di canali di comunicazione su linee dedicate, fisicamente o logicamente, o comunque su collegamenti basati su Virtual Private Network.

2. Attraverso i canali di cui al comma 1, si realizzano tutte le attività in carico alle procure previste dal codice di procedura penale, ivi comprese quelle svolte, per quanto di competenza dal procuratore della Repubblica, dall'ufficio che ha richiesto ed eseguito le intercettazioni nell'esercizio dei compiti di direzione e sorveglianza dell'archivio delle intercettazioni, oltre che di gestione e tenuta dello stesso.

Articolo 6

Disposizioni finali

1. I requisiti tecnici specifici di cui al presente decreto, previa verifica con cadenza annuale, sono soggetti a eventuali aggiornamenti periodici, in relazione all'evoluzione tecnologica dei sistemi e delle minacce nel contesto della cybersecurity e ai migliori e più aggiornati standard di sicurezza cibernetica. Ai fini di tali aggiornamenti è sentita l'Agenzia per la cybersicurezza nazionale.

2. Al fine di disporre l'attivazione di cui all'art. 2, comma 5, del decreto-legge 10 agosto 2023, n. 105, convertito con modificazioni dalla legge 9 ottobre 2023, n. 137, saranno dettagliate, con il decreto indicato nella medesima disposizione, ulteriori misure tecnico-organizzative di funzionamento del sistema.

3. Le misure tecnico-organizzative di cui al comma 2, da aggiornare periodicamente anche in base ad una valutazione d'impatto sulla protezione dei dati di cui all'articolo 23 del decreto legislativo 18 maggio 2018, n. 51, sono tali da garantire un livello di sicurezza adeguato al rischio potenzialmente connesso al trattamento, ai sensi dell'articolo 25 del citato decreto legislativo.

Il presente decreto verrà pubblicato nel Bollettino Ufficiale del Ministero della giustizia.

Roma,5 gennaio 2024

Il Ministro
CARLO NORDIO

ORDINI PROFESSIONALI E ALBI

Procedura di valutazione comparativa per il rilascio dell'autorizzazione allo svolgimento delle funzioni di Istituto Vendite Giudiziarie nell'ambito del circondario del Tribunale di Treviso.

Visti gli artt. 1, 2, 3, 10 e 40 del d.m. 11 febbraio 1997, n. 109;

Visto l'art. 159 disp. att. c.p.c.;

Visto il provvedimento della Direzione Generale degli Affari Interni – Ufficio II – Ordini professionali e albi (m_dg.DAG.06/40/2023.0200924.U) del 6/10/2023 di richiesta di un bando di gara nel circondario del Tribunale di Treviso, ex art. 3, comma 2, d.m. n. 109/1997 in ordine al rilascio di una seconda concessione per l'espletamento del servizio vendite giudiziarie;

Considerato il parere favorevole del Tribunale circa la necessità di un secondo concessionario, da affiancare a quello attuale, al fine di smaltire l'arretrato e di garantire un più efficiente svolgimento dell'attività;

Ritenuto di dover procedere al compimento degli atti necessari al rilascio dell'autorizzazione allo svolgimento delle funzioni di istituto vendite giudiziarie nell'ambito del suindicato circondario, pubblicando apposito avviso che consenta a tutti i soggetti interessati di presentare la propria istanza entro il termine fissato, corredata della documentazione necessaria alla verifica della sussistenza dei requisiti di idoneità e per la valutazione comparativa delle domande;

Ritenuto, in particolare, che la valutazione comparativa delle domande debba avvenire, previa verifica dei requisiti di idoneità, nel rispetto dei principi di pubblicità e di trasparenza dell'azione amministrativa;

Avvisa

1. È indetta una procedura di valutazione comparativa per il rilascio dell'autorizzazione allo svolgimento delle funzioni di istituto vendite giudiziarie nell'ambito del circondario del tribunale di Treviso.

2. La domanda di partecipazione dovrà essere presentata, in busta chiusa e sigillata con in evidenza i riferimenti della procedura come descritto al punto 9 del presente bando, entro il termine di 60 giorni dalla data di pubblicazione del presente avviso, a mezzo posta raccomandata con ricevuta di ritorno ovvero mediante consegna presso la segreteria della Presidenza della Corte di Appello di Venezia.

3. La domanda dovrà indicare:

a) le generalità del richiedente, ovvero, se persona giuridica, la denominazione sociale, la data di costituzione e le generalità dell'amministratore o dei componenti del consiglio di amministrazione;

b) la residenza o il domicilio del richiedente ovvero, se persona giuridica, la sede legale;

c) in caso di persona giuridica, l'oggetto sociale, la durata della carica degli organi di amministrazione nonché il numero e le generalità dei soci;

d) la denominazione con la quale si intende esercitare il servizio;

e) il luogo ove l'istituto intende avere i propri uffici per lo svolgimento del servizio;

f) i propri recapiti (telefono, posta elettronica, posta elettronica certificata).

4. Alla domanda, inoltre, dovranno essere allegati i seguenti documenti:

a) in caso di persona giuridica, la copia conforme dell'atto costitutivo e dello statuto;