**Anno CXLV - Numero 6**

**Roma, 31 marzo 2024**

*Pubblicato il 2 aprile 2024*

# BOLLETTINO UFFICIALE del Ministero della Giustizia

PUBBLICAZIONE QUINDICINALE

# PARTE PRIMA
## DISPOSIZIONI GENERALI

**Decreto Ministeriale 15 marzo 2024 – Ai sensi dell'art. 1, comma 2, del d.lgs. 4 maggio 2023 n. 54, istituzione dell'archivio nazionale dei verbali, degli atti e delle registrazioni delle intercettazioni eseguite nei procedimenti in cui la Procura europea ha esercitato la sua competenza, nonché di ogni altro atto ad esse relativo.**

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'art. 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 regolamento (UE) 2017/1939 del consiglio del 12 ottobre 2017 relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea (EPPO);

Visto il decreto legislativo 2 febbraio 2021, n. 9, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea (EPPO);

Visto il decreto legislativo 4 maggio 2023, n. 54 recante disposizioni integrative e correttive del decreto legislativo 2 febbraio 2021, n. 9;

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

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

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 cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (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 Procuratore capo europeo e il Garante per la protezione dei dati personali;

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, quali alterazione, cancellazione o aggiunta, attraverso meccanismi di checksum, tecniche crittografiche, ovvero meccanismi per il controllo dell'accesso ai dati;

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) «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;

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

f) «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;

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

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

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

l) «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;

m) «crittografia dei dati at-rest»: applicazione di algoritmi crittografici al fine di cifrare dati e informazioni memorizzati su dispositivi di archiviazione non volatili, con l'obiettivo di garantire la riservatezza delle informazioni non soltanto quando i dati

vengono utilizzati ma anche quando essi sono "a riposo" (at-rest), ossia quando i supporti fisici su cui sono memorizzati sono spenti o accesi ma inutilizzati;

n) «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'art. 24 del decreto legislativo del 7 marzo 2005 n. 82;

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

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

q) «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;

r) «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;

s) «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;

t) «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;

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

v) «attacco brute force»: in crittografia, metodo che si utilizza per trovare la chiave di un sistema, ad esempio provando tutte le possibili combinazioni o attraverso l'utilizzo di un dizionario;

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

aa) «Active Directory (AD)»: servizio che archivia le informazioni relative agli oggetti sulla rete e semplifica la ricerca e l'uso di queste informazioni da parte degli amministratori e degli utenti;

bb) «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;

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

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

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

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

gg) «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;

hh) «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.

Articolo 2

*Oggetto e ambito di applicazione*

1. Ai sensi dell'art. 1, comma 2 del decreto legislativo 4 maggio 2023, n. 54 è istituito l'archivio nazionale dei verbali, degli atti e delle registrazioni delle intercettazioni eseguite nei procedimenti in cui la Procura europea ha esercitato la sua competenza, nonché di ogni altro atto ad esse relativo, di seguito denominato «archivio».

2. L'archivio è tenuto sotto la direzione e la sorveglianza esclusive del procuratore europeo o, nei casi previsti dall'articolo 16, paragrafo 7, del regolamento (UE) 2017/1939 del Consiglio, del 2 ottobre 2017, dal procuratore europeo delegato nominato quale sostituto del procuratore europeo dal collegio della Procura europea.

3. Ai fini della definizione dei requisiti tecnici specifici dell'archivio, si tiene conto che:

a) il processo di conferimento prevede 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 prevede 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) nel caso di trasferimento del procedimento verso ufficio giudiziario diverso da quello che ha disposto ed eseguito le intercettazioni, il trasferimento delle intercettazioni svolte avviene mediante il 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, è previsto 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 sono realizzati in modo da garantire la gestione sia degli eventi e dati costituenti nuove intercettazioni sia di quelli già presenti ma non ancora 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 – è conservato 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 europeo 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.

Articolo 3
*Infrastrutture digitali e sistemi di ripristino*

1. L'archivio utilizza le infrastrutture digitali interdistrettuali di cui all'articolo 2, comma 1, del decreto-legge 10 agosto 2023, n. 105. Tali infrastrutture assicurano la memorizzazione di tutte le conversazioni e comunicazioni registrate a mezzo degli impianti degli uffici di procura nell'ambito di un procedimento penale in cui la Procura europea ha esercitato la sua competenza, nonché di ogni altro atto ad esse relativo. Le infrastrutture digitali interdistrettuali potranno inoltre essere attrezzate per le operazioni di intercettazione secondo l'evoluzione tecnologica.

2. Le infrastrutture digitali interdistrettuali sono quattro e sono installate in sale interdistrettuali collocate nel distretto della Corte d'appello di Milano, della Corte d'appello di Roma, della Corte d'appello di Napoli e della Corte d'appello di Palermo.

3. I sistemi di ripristino sono nativamente integrati all'interno della piattaforma tecnologica di memorizzazione dei dati operativa presso le infrastrutture digitali interdistrettuali. 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.

4. La piattaforma tecnologica di memorizzazione dei dati operativa presso le infrastrutture digitali interdistrettuali prevede meccanismi atti a rilevare, tramite specifici alert, comportamenti anomali o rischi che possono compromettere la continuità operativa o la piena funzionalità della piattaforma. Sono inoltre previsti audit con cadenza almeno annuale per la valutazione periodica dell'adeguatezza delle misure e la verifica a posteriori, a campione ovvero a seguito di alert, della legittimità delle operazioni effettuate.

5. L'archivio, attraverso le infrastrutture digitali interdistrettuali, rispetta i requisiti di sicurezza di tutti i dati ivi memorizzati, vale a dire garantisce la loro riservatezza, integrità, autenticità e disponibilità.

Articolo 4
*Trasmissione dei dati all'archivio*

1. Le conversazioni e comunicazioni registrate nell'ambito di un procedimento penale sono trasmesse con modalità esclusivamente telematiche, alle infrastrutture digitali di cui all'articolo 3, comma 1, per essere conservate nell'archivio.

2. Il collegamento telematico di cui al comma 1 del presente articolo è realizzato mediante canali sicuri, ove i dati transitano in forma cifrata. I canali suddetti garantiscono inoltre l'integrità dei dati mediante appositi meccanismi per rilevare qualsiasi indebita modifica sulle informazioni in transito.

3. I dati conferiti, contenenti le conversazioni e comunicazioni registrate, vengono inviati cifrati tramite canale di comunicazione cifrato mediante l'utilizzo di tecniche crittografiche allo stato dell'arte per la protezione dei dati "in transito", anche tenendo conto di eventuali raccomandazioni fornite dall'Agenzia per la cybersicurezza nazionale. Il canale di comunicazione garantisce la autenticazione degli attori coinvolti e implementa meccanismi per assicurare l'integrità e autenticità delle comunicazioni.

4. I dati vengono memorizzati nell'archivio in un'area logica univoca e distinta.

5. Le apparecchiature presenti in ciascuna delle sale interdistrettuali di cui all'articolo 3, comma 2, ricevono i dati conferiti, applicano un ulteriore strato di cifratura e li distribuiscono sullo storage in modo tale da garantire la massima disponibilità dei dati stessi.

Articolo 5
*Autenticità e integrità dei dati*

1. Ai fini di assicurare l'autenticità e l'integrità dei dati 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 che possa incidere sulla funzionalità dei sistemi è preceduto da una interlocuzione con il procuratore europeo e con il procuratore europeo delegato. Sono assicurate in ogni caso la tracciabilità e la immediata e diretta conoscibilità da parte del procuratore europeo e del procuratore europeo delegato 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 6
*Riservatezza dei dati*

1. Ai fini di assicurare la riservatezza e la sicurezza dei dati contenuti nell'archivio, sono adottate le pratiche di sicurezza informatica previste per la protezione dei dati da usi impropri, quali crittografia e restrizioni di accesso, sia fisiche sia digitali.

2. Tutti gli eventi costituenti le intercettazioni sono contenuti in un file contenitore criptato mediante un algoritmo simmetrico caratterizzato da elevata resistenza ad attacchi di tipo brute force.

3. La chiave simmetrica utilizzata come input dell'algoritmo di cui al comma 2 del presente articolo deve essere trasmessa alla Procura europea garantendone la segretezza attraverso un processo di ulteriore cifratura della stessa.

4. L'area logica di cui all'articolo 4 comma 4 del presente decreto garantisce la cifratura di tutti i dati at-rest, anche tenendo conto di eventuali raccomandazioni fornite dall'Agenzia per la cybersicurezza nazionale

5. Le infrastrutture digitali interdistrettuali sono organizzate in modo da garantire la sicurezza fisica delle apparecchiature che compongono l'archivio. Gli accessi fisici agli ambienti ove sono installati i componenti dell'archivio sono regolamentati mediante un registro degli accessi.

6. Gli accessi amministrativi ai vari componenti dell'archivio sono regolamentati e protetti da autenticazione a due fattori e da un sistema di log che consenta di ricostruire tutte le operazioni effettuate in modo da tracciare in maniera non modificabile le azioni di chi svolge attività di tipo sistemistico e manutentivo, in conformità a quanto previsto dagli artt. 21 del decreto legislativo 18 maggio 2018, n. 51 e 89-bis, comma 3, ultimo periodo, delle disposizioni attuative del codice di procedura penale.

7. I sistemi informatici costituenti le infrastrutture digitali interdistrettuali non hanno accesso ai dati in chiaro delle intercettazioni, poiché li ricevono in forma già cifrata, né hanno accesso alla chiave di decifratura. Presso le infrastrutture digitali interdistrettuali sono presenti in chiaro solo i metadati che non contengono informazioni sensibili e devono necessariamente rimanere in chiaro per il corretto funzionamento del sistema.

8. 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.

9. 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.

10. La piattaforma di cui al comma 5 garantisce il controllo e la centralizzazione di identità, gruppi, policy e configurazioni. La piattaforma riconosce e gestisce tutte le utenze censite all'interno della foresta Active Directory Nazionale che contiene i riferimenti del personale interno al Ministero di Giustizia. Inoltre, 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.

11. 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 Connecti 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) utilizzo di autenticazione a due fattori con credenziali e dispositivi di autenticazione assegnati all'utente, anche tenendo conto di eventuali raccomandazioni fornite dall'Agenzia per la cybersicurezza nazionale;

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

f) 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.

12. La piattaforma di cui al comma 5 garantisce, attraverso un sistema di log, il tracciamento in maniera non modificabile di tutte le operazioni compiute dagli utenti e l'identificazione univoca delle operazioni stesse, in conformità a quanto previsto dagli artt. 21 del decreto legislativo 18 maggio 2018, n. 51 e 89-bis, comma 3, ultimo periodo, delle disposizioni attuative del codice di procedura penale.

Articolo 7
*Collegamento telematico tra l'archivio e le sedi dei procuratori europei delegati*

1. Il collegamento telematico tra l'archivio e gli impianti installati presso gli uffici di procura indicati all'articolo 10 del decreto legislativo 2 febbraio 2021, n. 9, 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 dalla normativa vigente in materia di intercettazioni disposte nei procedimenti di competenza della Procura europea, ivi comprese quelle svolte dal procuratore europeo o, nei casi previsti dall'articolo 16, paragrafo 7, del regolamento (UE) 2017/1939 del Consiglio, del 2 ottobre 2017, dal procuratore europeo delegato nominato quale sostituto dal collegio della Procura europea, nell'esercizio dei compiti di direzione e sorveglianza dell'archivio delle intercettazioni, oltre che di gestione e tenuta dello stesso.

3. Ai fini indicati dal comma 2, il processo di conferimento di cui all'articolo 2, comma 3, lettera a), e il processo di consultazione di cui all'articolo 2, comma 3, lettera b), sono assicurati presso ciascuna delle procure distrettuali individuate quali sede di servizio dei procuratori europei delegati, anche se diverse dall'ufficio presso cui si trovano le postazioni utilizzate per l'esecuzione delle operazioni di intercettazione.

Articolo 8
*Trattamento dei dati personali*

1. Nell'ambito dei procedimenti che richiedono l'esecuzione di intercettazioni nei casi previsti dal codice di procedura penale, il Ministero della Giustizia realizza il trattamento di dati ai soli fini dell'allestimento e della manutenzione delle infrastrutture digitali interdistrettuali, comprendente l'attivazione del nuovo archivio centralizzato, garantendo l'autonomia del procuratore europeo o, nei casi previsti dall'articolo 16, paragrafo 7, del regolamento (UE) 2017/1939 del Consiglio, del 2 ottobre 2017, dal procuratore europeo delegato nominato quale sostituto del procuratore europeo dal collegio della Procura europea, nell'esercizio delle funzioni di direzione, organizzazione e sorveglianza sulle attività di intercettazione e sui relativi dati e, in ogni caso, con esclusione dell'accesso ai dati in chiaro.

2. Il trattamento di dati è svolto al fine di assicurare i più elevati e uniformi livelli di sicurezza, aggiornamento tecnologico, efficienza, economicità e capacità di risparmio energetico dei sistemi informativi funzionali alle attività di intercettazione eseguite da ciascun ufficio del pubblico ministero, consentendo alla Procura europea il perseguimento delle seguenti finalità:

a) conferimento o trasferimento degli eventi e dei metadati che costituiscono le intercettazioni nel nuovo archivio centralizzato, in grado di garantire una maggiore efficienza nella gestione delle risorse;

b) consultazione delle intercettazioni da parte del giudice che procede e i suoi ausiliari, il pubblico ministero e i suoi ausiliari, ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto, i difensori delle parti, assistiti, se necessario, da un interprete, ai sensi dell'art. 89-bis, comma 3, delle disposizioni di attuazione del codice di procedura penale;

c) consultazione delle intercettazioni da parte dei difensori delle parti, successivamente alla notifica del deposito delle stesse presso il nuovo archivio centralizzato, al fine di valutare il contenuto delle intercettazioni nell'interesse degli assistiti, ai sensi dell'art. 89-bis, comma 5, delle disposizioni di attuazione del codice di procedura;

d) rilascio di copie delle intercettazioni a beneficio dei difensori o di eventuali altri uffici giudiziari autorizzati all'accesso ai contenuti, consentendo la consultazione dei contenuti in un secondo momento, a norma degli articoli 268, 415-bis e 454 del codice di procedura penale;

e) trasferimento per competenza verso altra procura, anche contestualmente al conferimento dell'intercettazione, nel caso in cui la competenza di una determinata indagine passi ad una diversa procura.

3. Il Ministero della Giustizia è responsabile del trattamento di dati personali effettuati nell'ambito dell'allestimento e della manutenzione delle infrastrutture digitali interdistrettuali per le intercettazioni per conto della Procura europea ai sensi del dell'articolo 18 del decreto legislativo 18 maggio 2018, n. 51.

4. Il Ministero della Giustizia si avvale di soggetti fornitori di tecnologie e servizi funzionali all'allestimento e alla manutenzione delle infrastrutture digitali interdistrettuali per le intercettazioni, sulla base di quanto disposto dell'articolo 18, commi 2 e 3, lettera f), del decreto legislativo 18 maggio 2018, n. 51, tra cui:

a) gestione e manutenzione del servizio identity management del Ministero della Giustizia;

b) gestione e manutenzione dei database;

c) gestione e conduzione applicativa;

d) manutenzione della soluzione di conservazione centralizzata delle intercettazioni per ciò che concerne le componenti ospitate presso le infrastrutture digitali interdistrettuali;

e) installazione e gestione degli apparati di rete nell'ambito delle infrastrutture digitali interdistrettuali;

f) gestione dei firewall di rete presso le infrastrutture digitali interdistrettuali;

g) gestione e manutenzione delle componenti hardware e software installati presso le sedi della Procura europea, inclusi

eventuali apparati di rete, atti ad interfacciarsi sia con i fornitori dei servizi di intercettazione sia con il sistema soluzione di conservazione centralizzata, nell'ambito delle finalità di trattamento di dati perseguite dalla Procura europea.

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

Roma, 15 marzo 2024

*Il Ministro*
CARLO NORDIO

## ORDINI PROFESSIONALI E ALBI

**Indizione bando di gara per la procedura di valutazione comparativa per il rilascio dell'autorizzazione allo svolgimento delle funzioni di Istituto di Vendite Giudiziarie per i circondari dei Tribunali di Catania, Ragusa e Caltagirone.**

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 decreto del Direttore generale della giustizia civile del 12 novembre 2003, con il quale l'Ente I.V.G. Istituto Vendite Giudiziarie s.r.l. era stato autorizzato allo svolgimento delle funzioni di istituto vendite giudiziarie – e dunque alla vendita all'incanto di beni mobili disposta dall'autorità giudiziaria, di custodia di beni mobili e di amministrazione giudiziaria dei beni immobili – nell'ambito dei circondari dei Tribunali di Catania, Ragusa e Caltagirone;

Considerata la revoca di tale autorizzazione in data 15 ottobre 2021, pubblicata sul Bollettino ufficiale del Ministero della giustizia n.21 del 15 novembre 2021;

Ritenuto di dover procedere al compimento degli atti necessari al rilascio dell'autorizzazione allo svolgimento delle funzioni di istituto vendite giudiziarie nell'ambito dei suindicati circondari, 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 dei Tribunali di Catania, Ragusa e Caltagirone.

2. La domanda di partecipazione dovrà essere presentata, in busta chiusa e sigillata con in evidenza i riferimenti della procedura e l'indirizzo pec del mittente, 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.

Al fine di evitare che la busta venga erroneamente aperta prima della consegna all'ufficio interessato, si invita ad inserire la busta contenente la domanda di partecipazione in un'ulteriore busta che contenga all'esterno i medesimi dati della prima.

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;

b) il certificato penale e il certificato dei carichi pendenti del richiedente ovvero, in caso di persona giuridica, dell'amministratore o dei componenti del consiglio di amministrazione;

c) la documentazione relativa alla capacità patrimoniale del richiedente ovvero, nel caso di persona giuridica, copia conforme dei bilanci dell'ultimo triennio;

d) una dichiarazione di responsabilità circa l'assenza di cause di incompatibilità;

e) la certificazione antimafia.

5. Al fine di consentire la valutazione della sussistenza dei requisiti di idoneità allo svolgimento del servizio, alla domanda dovrà essere altresì allegato il progetto organizzativo e gestionale che si intende realizzare, con specifica indicazione:

a) dei locali, delle attrezzature e degli automezzi da destinare allo svolgimento del servizio oggetto della presente procedura, con indicazione del titolo giuridico in base al quale si avrà la disponibilità degli stessi;

b) delle unità di personale da impiegare nello svolgimento del servizio, con indicazione della relativa tipologia contrattuale;

c) dell'esistenza di eventuali incarichi identici o analoghi svolti o in corso di svolgimento nei circondari di altri tribunali.

6. Al fine di comprovare la sussistenza dei predetti requisiti, le dichiarazioni ad essi relative dovranno essere redatte con la espressa e consapevole menzione delle sanzioni di legge in caso di dichiarazioni mendaci ai sensi del d.p.r. 28 dicembre 2000, n. 445, e con espressa assunzione di responsabilità da parte del dichiarante.

7. In presenza di domande presentate da più soggetti astrattamente idonei a svolgere il servizio, costituiranno elementi preferenziali:

a) la disponibilità di maggiori strutture e mezzi da destinare al servizio oggetto della presente procedura;

b) la disponibilità di apposita piattaforma informatica per la gestione delle vendite con modalità telematiche (art. 161-ter disp. att. c.p.c; d.m. 26 febbraio 2015, n. 32) e la specifica esperienza maturata in tale ambito;

c) la maggiore solidità economica e finanziaria.

8. Verrà data notizia del giorno e dell'ora dell'apertura delle buste ai partecipanti che ne faranno richiesta all'indirizzo mail prot.ca.catania@giustiziacert.it.