Ministero della Giustizia

Ministero dell'Interno

Visti gli articoli 14, commi 5 e 8, e 35-*bis*, commi 8 e 16, del decreto legislativo 28 gennaio 2008, n.25 recante "Attuazione della direttiva 2005/85/CE recante norme minime per le procedure applicate negli Stati membri ai fini del riconoscimento e della revoca dello status di rifugiato", che prevedono l'adozione di un decreto direttoriale per l'individuazione delle specifiche tecniche per la messa a disposizione, nella fase giurisdizionale di merito, della videoregistrazione del colloquio del richiedente asilo;

Visto il decreto legislativo 7 marzo 2005, n.82, recante "Codice dell'Amministrazione Digitale";

Visto il decreto del Ministro della giustizia 31 marzo 2011, n.44 recante Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005;

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

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);

Sentito il Garante per la protezione dei dati personali che si è espresso con provvedimento n.466 del 18 luglio 2024, trasmesso con nota n DAGES/MCC/262113.

D'INTESA
ADOTTANO IL SEGUENTE
DECRETO DIRETTORIALE

ART. 1
(*Oggetto*)

1. Il presente decreto stabilisce le modalità tecniche per la messa a disposizione del giudice e dei soggetti abilitati ai sensi dell'articolo 4, da parte delle Commissioni territoriali e delle Sezioni per il riconoscimento della protezione internazionale o da parte della Commissione Nazionale per il Diritto di Asilo, per il tramite del DLCI-Ministero dell'interno della videoregistrazione del colloquio del richiedente asilo.

ART. 2

(*Definizioni*)

1. Ai fini del presente provvedimento si intende per:

a) ADDETTI UPP: le persone assegnate all'ufficio per il processo costituito presso il Tribunale presso il quale sono istituite le sezioni specializzate dei Tribunali ordinari che si occupano di immigrazione, protezione internazionale e libera circolazione dei cittadini dell'Unione europea istituite ai sensi dell'articolo 1, decreto-legge 17 febbraio 2017, n.13 (convertito, con modificazioni, con legge 13 aprile 2017. N.46);

b) ARCHIVIAZIONE: processo di memorizzazione sistematica della registrazione audio-video dell'audizione del richiedente asilo all'interno di uno spazio digitale tale (storage) che tali elementi rimangano presenti e integri in modo ordinato e non casuale per poter essere facilmente accessibili ed utilizzabili per un uso futuro. All'interno dello storage di S.IN.D.A.C.A. tali requisiti di integrità e disponibilità sono garantiti da software dedicato (attualmente HCP);

c) ASR CLIENT: applicazione installata sulle postazioni di lavoro periferiche del sistema S.IN.D.A.C.A. collocate presso le Commissioni e le Sezioni territoriali per il riconoscimento della protezione internazionale che inviano i frame audio-video dell'audizione e riceve la relativa trascrizione effettuata dal server centrale ove è installato il motore ASR;

d) ASR SERVER: applicazione installata sul server centrale del sistema S.IN.D.A.C.A. che riceve i frame audio video dai Client collocati consente il colloquio con il server centrale ove è installato;

e) CAD: Codice per l'Amministrazione Digitale, di cui al testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese, adottato con decreto legislativo 7 marzo 2005 n. 82 e ss. mm;

f) CANCELLERIA: la cancelleria delle sezioni specializzate istituite presso i Tribunali ordinari ai sensi dell'articolo 1, decreto-legge 17 febbraio 2017, n.13 (convertito, con modificazioni, con legge 13 aprile 2017. n.46);

g) CED: il Centro Elaborazione Dati del Dipartimento per le Libertà Civili e l'Immigrazione del Ministero dell'Interno;

h) Codice CUI: il codice univoco identità assegnato in fase di riconoscimento del cittadino di paese terzo o apolide assegnato dal sistema AFIS;

i) COMMISSIONE NAZIONALE: COMMISSIONE NAZIONALE PER IL DIRITTO D'ASILO, l'Autorità di riferimento del sistema italiano di protezione internazionale, dotata di compiti di indirizzo e coordinamento delle Commissioni e delle Sezioni territoriali per il riconoscimento della protezione internazionale, che sono i collegi competenti per il riconoscimento delle varie forme di protezione internazionale. Ha inoltre competenze decisionali in materia di eventuale revoca e cessazione delle forme di protezione già riconosciute dai suddetti organismi;

l) COLLEGI TERRITORIALI: COMMISSIONI E SEZIONI TERRITORIALI PER IL RICONOSCIMENTO DELLA PROTEZIONE INTERNAZIONALE, articolazioni territoriali del Sistema Asilo che si occupano con poteri decisionali delle domande di riconoscimento della protezione internazionale;

m) DLCI -MINISTERO DELL'INTERNO: il Dipartimento per le Libertà Civili e l'Immigrazione del Ministero dell'Interno, articolazione del Ministero dell'Interno presso cui risultano incardinate la Commissione Nazionale per il Diritto di asilo e l'Ufficio II- Ufficio informatico;

n) MINISTERO DELL'INTERNO : il Ministero dell'interno ai sensi dell'articolo 3 D.M. del 15 dicembre 2023 è il titolare del trattamento dei dati personali nel proprio ambito di competenza e lo esercita ex art.3, comma 3 lett.b) tramite i Capi Dipartimento;

o) HCP: (*Hitachi Content Platform*) soluzione tecnologica che viene attualmente utilizzata nello storage S.IN.D.A.C.A. per assicurare il rispetto dei criteri di archiviazione richiesti dalla normativa in vigore;

p) HTTPS: *(HyperText Transfer Protocol over Securesocketlayer)* indica il protocollo di accesso alle informazioni fruibili sul World Wide WEB. La lettera S indica la versione del protocollo http che utilizza un canale di trasporto cifrato per esempio SSL (SecureSocketLayer) o Transport Security Layer(TLS);

q) IPT: *(Information Technology)* Tecnologie riguardanti i sistemi,le apparecchiature, i server e i sistemi interconnessi di apparecchiature utilizzati per l'acquisizione, l'archiviazione, l'elaborazione, la gestione, il controllo, la visualizzazione di dati o informazioni;

r) ICT: ***(****Information e Communication Technology)* Tecnologie riguardanti le apparecchiature, i server e i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili),

le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare dati e informazioni;

s) LAN: *(Local Area Network)* rete informatica estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come una porzione di edificio, un edificio o un complesso di edifici adiacenti;

t) MOTORE ASR: *(Automatic Speech Recognition)* applicazione basata su tecnologia Client/Server che consente il riconoscimento automatico del parlato naturale della lingua italiana, l'indicizzazione dei singoli frame audio-video e la relativa trascrizione;

u) PCT: il processo civile telematico come regolato dal decreto del Ministro della giustizia 31 marzo 2011, n.44;

v) ReGIndE: il registro generale degli indirizzi elettronici, come definito all'art. 7 del Regolamento DM 21 febbraio 2011, n.44;

z) RETE INTRANET: rete privata dedicata alla interconnessione delle amministrazioni e degli enti pubblici nazionali;

aa) SAML: *(Security Assertion Markup Language)* standard di federazione aperto che consente una comunicazione sicura tra più domini e tra il cloud pubblico e altri sistemi abilitati trasferendo il Token di autenticazione a un'altra applicazione, e che svolge due principali funzioni di sicurezza: 1) l'autenticazione che consiste nella conferma dell'identità degli utenti; 2) l'autorizzazione che è un passaggio dell'autorizzazione utente alle applicazioni per l'accesso a determinati sistemi o contenuti;

bb) SERVER: dispositivo o sistema informatico connesso in rete, pubblica o privata, che consente di utilizzare le risorse condivise dallo stesso (dati, programmi, hardware), da parte di ulteriori dispositivi o sistemi informati chiamati client che si connettono alla rete;

cc) SPC- Sistema Pubblico di Connettività: ~~i~~nsieme di regole tecniche e di principi che definisce le modalità preferenziali che i sistemi informativi delle pubbliche amministrazioni devono adottare per essere tra loro interoperabili. È la cornice nazionale di interoperabilità;

dd) SEZIONE SPECIALIZZATA: la sezione specializzata dei Tribunali ordinari in materia di immigrazione, protezione internazionale e libera circolazione dei cittadini dell'Unione europea istituita ai sensi dell'articolo 1, decreto-legge 17 febbraio 2017, n.13 (convertito, con modificazioni, con legge 13 aprile 2017. n.46);

ee) S.IN.D.A.C.A.*(Sistema Informativo di documentazione delle Audizioni delle Commissioni Asilo)*: il sistema informatico utilizzato per la videoregistrazione delle audizioni dei richiedenti protezione internazionale e per la trascrizione della relativa verbalizzazione, mediante riconoscimento automatico del parlato;

ff) SLA (*Service Level Agreement):* sono i livelli di servizio che vengono garantiti in termini di accessibilità e disponibilità del servizio IT;

gg) TECNOLOGIA BLADE SERVER: dispositivo hardware pensato per minimizzare l'occupazione di spazio. I server Blade tipicamente un server (fisico) distinto che singolarmente o in concorso con altre lame, può simulare N macchine server virtuali;

hh) TECNOLOGIA STORAGE: si identificano i dispositivi hardware, i supporti per la memorizzazione, le infrastrutture ed i software dedicati alla memorizzazione non volatile di grandi quantità di informazioni in formato elettronico;

ii) TLS: *(Transport Security Layer)* protocollo crittografico che permette una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti, come ad esempio Internet, fornendo autenticazione, integrità dei dati e confidenzialità;

ll) TOKEN: struttura dati funzionale alla fase di accreditamento dei soggetti autorizzati ad accedere con le diverse modalità previste ai file archiviati nel sistema S.IN.D.A.C.A. ;

mm) URL: *Uniform Resource Locator* è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete pubblica o privata;

nn) VESTA.NET*(Verifica Status)*: applicazione web pubblicata sulle reti intranet, dedicate alla gestione delle istanze di protezione internazionale, ad uso esclusivo degli utenti delle Commissioni Territoriali per il riconoscimento della protezione internazionale e relative Sezioni e della Commissione Nazionale per il Diritto di Asilo;

oo) WEB SERVICE: Servizi Web fruibili sia in modalità Client To Server sia in modalità Server To Server. I servizi possono essere erogati tramite specifici web server o application server mediante l'utilizzo di protocolli HTTPS;

pp) XSD: file scritto nel linguaggio dello schema XML, utilizzato per definire quali elementi e attributi possono apparire in un documento XML che definisce anche la relazione degli elementi e quali dati possono essere memorizzati in essi;

qq) XML: *(eXtensible Markup Language)* metalinguaggio basato su un meccanismo sintattico di marcatori (markup), fatto da una serie di istruzioni (tag), che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo e permette di creare documenti e dati strutturati in formato elettronico.

ART. 3

(Il *sistema S.IN.D.A.C.A.*)

1. Il sistema S.IN.D.A.C.A. consente ai Collegi territoriali e alla Commissione Nazionale di procedere alla videoregistrazione e alla trascrizione del verbale di audizione del richiedente asilo.
2. Detto sistema si compone di:

a) un motore applicativo ASR Client per l'acquisizione dei file video e audio, la successiva visualizzazione ed eventuale modifica o integrazione;
b) un motore applicativo ASR Server per l'elaborazione dei file video e audio per il riconoscimento automatico del parlato naturale della lingua italiana e la trasmissione della trascrizione dell'audizione al Client;
c) apparati Server con tecnologia *blade* e *storage* di grande capacità necessari per l'installazione dell'applicativo ASR lato Server e l'archiviazione di tutti i file video, audio, delle relative trascrizioni e di ogni altra documentazione raccolta durante le audizioni;
d) un portale dedicato per consentire l'accesso ai file archiviati agli utenti accreditati al sistema in funzione dei rispettivi ruoli e funzioni .

3. Il DLCI- Ministero dell'interno gestisce, attraverso apposite infrastrutture tecniche, l'archiviazione della videoregistrazione del colloquio del richiedente protezione internazionale e del relativo verbale di audizione nei propri CED dipartimentali garantendone l'integrità, la conservazione e la disponibilità dei dati .

ART. 4

(*Procedura e specifiche tecniche per la messa a disposizione del giudice della videoregistrazione del colloquio del richiedente asilo e per l'accesso alla predetta videoregistrazione da parte dei soggetti abilitati)*

1. Ai sensi dell'articolo 35-bis, comma 8, del decreto legislativo n.25 del 2008, sono

abilitati ad accedere alla videoregistrazione del colloquio del richiedente asilo, secondo le modalità indicate dal presente articolo:

a) l'avvocato del richiedente asilo munito di procura debitamente verificata dalla cancelleria competente;

b) ciascun magistrato della sezione specializzata avanti alla quale è stato presentato il ricorso contro la decisione dei Collegi territoriali o della Commissione nazionale;

c) i cancellieri e gli addetti UPP della sezione specializzata cui appartengono i magistrati di cui alla lettera b);

2. Dopo la notifica all'interessato del provvedimento di diniego adottato dai Collegi territoriali, l'avvocato del richiedente asilo, munito di procura, richiede alla cancelleria della sezione specializzata competente l'accesso alla videoregistrazione. La cancelleria, previa verifica della procura, invia, mediante *web service,* il pacchetto informativo contenente i dati necessari al DLCI-Ministero dell'interno, che, in conformità alle specifiche riportate nell'allegato tecnico, nella sezione denominata "Accesso dei soggetti abilitati", assicura l'accesso attraverso il collegamento ad una apposita pagina web dedicata, a seguito di verifica della corrispondenza con i dati del pacchetto informativo.
3. Dopo il deposito del ricorso, la videoregistrazione del colloquio del richiedente asilo è resa disponibile al difensore, se diverso dall'avvocato di cui al comma 2, secondo le modalità previste dal comma 2.
4. La messa a disposizione della videoregistrazione ai soggetti di cui al comma 1 lettere b) e c) è assicurata mediante l'accesso all'applicazione S.IN.D.A.C.A., tramite rete InfranetSPC, attraverso una URL pubblicata dal Ministero della giustizia, secondo le specifiche indicate nell'allegato tecnico, nella sezione "Accesso dei soggetti abilitati". DLCI- Ministero dell'interno, acquisito il pacchetto informativo da parte della cancelleria e verificata la corrispondenza delle informazioni inviate con i dati inseriti nel sistema S.IN.D.A.C.A. in fase di autenticazione, consente l'accesso all'applicazione per la consultazione della videoregistrazione relativa al richiedente asilo ricorrente.
5. La cancelleria, non appena ne viene a conoscenza, comunica senza indugio al DLCI-Ministero dell'interno la cessazione, per qualsiasi causa, del mandato conferito all'avvocato autorizzato ai sensi dei commi 2 e 3.
6. I requisiti di sicurezza e protezione dei dati relativi al flusso di informazioni tra le cancellerie e il Ministero dell'interno e delle modalità di collegamento al portale S.IN.D.A.C.A e accesso alla videoregistrazione sono specificati nella sezione dell'allegato tecnico denominata "Descrizione requisiti di sicurezza".

ART. 5
(*Trattamento dati*)

1. Il Ministero dell'interno, l'ufficio giudiziario cui appartengono le sezioni specializzate e l'avvocato del richiedente asilo, sono titolari dei trattamenti da ciascuno effettuati sui dati personali conferiti da terzi o di propria pertinenza nell'ambito delle attività necessarie ai fini dell'applicazione del presente decreto.
2. Il Ministero dell'interno è titolare dei trattamenti dei dati personali effettuati mediante il sistema S.IN.D.A.C.A. e assicura che tali trattamenti avvengano adottando le misure necessarie a garantire il rispetto dei principi di liceità, correttezza e trasparenza nei confronti degli interessati, di limitazione della finalità, di minimizzazione dei dati, di limitazione della conservazione e di integrità e riservatezza e di protezione dei dati fin dalla progettazione e per impostazione predefinita in conformità agli articoli 5 e 25 del Regolamento (UE) 2016/679.
A tal fine, il Ministero dell'interno, adotta le misure di sicurezza tecniche e organizzative adeguate ai rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali, nel rispetto dell'articolo 32 del Regolamento (UE) 2016/679.
Tali misure sono state definite nella valutazione di impatto effettuata ai sensi dell'articolo 35 del Regolamento (UE) 2016/679 e comprendono, tra le altre:
a) la registrazione degli accessi e delle operazioni effettuate sul sistema S.IN.D.A.C.A., sulla videoregistrazione e sul relativo verbale da parte dei soggetti autorizzati, ai fini della verifica della liceità dei trattamenti, per finalità di controllo interno e per garantire l'integrità e la riservatezza dei dati personali. In particolare le registrazioni devono essere inviate e collezionate da un sistema informatico centralizzato che ne garantisca la correttezza, la completezza e la immodificabilità, con tempi di conservazione di 24 mesi**;**
b) l'utilizzo della crittografia per la protezione dei dati oggetto di trasmissione e di misure tecniche per garantire l'integrità, la non modificabilità e la certezza temporale dei dati registrati nei sottosistemi di memorizzazione del sistema S.IN.D.A.C.A.;
c) l'adozione di procedure operative**,** che coinvolgano i diversi titolari del trattamento, per rilevare e gestire eventuali violazioni dei dati personali, in accordo a quanto previsto dal Regolamento (UE) 2016/679 e dalle Linee guida 9/2022, v.2, sulla notifica delle violazioni dei dati personali adottate dall'European Data Protection Board (EDPB) il 28 marzo 2023;
d) la limitazione degli attributi associati alle identità digitali degli utenti del sistema S.IN.D.A.C.A., acquisiti nell'ambito delle procedure di autenticazione informatica, ai dati strettamente necessari;
e) le misure in relazione al trattamento dei dati personali necessari ai fini dell'espletamento delle verifiche e dei controlli da effettuarsi ai sensi del presente decreto;
f) le misure adottate per garantire un accesso selettivo alle informazioni da parte dei soggetti autorizzati e le altre misure poste a tutela dei diritti e delle libertà degli interessati.

3. Le misure tecniche e organizzative, definite nella valutazione d'impatto, sono riesaminate e aggiornate con cadenza almeno annuale o a seguito di modifica dei rischi relativi alla protezione dei dati derivanti da eventi quali: cambiamenti delle attività di trattamento, rilevazione di nuove minacce e vulnerabilità o variazioni dei sistemi informatici a supporto.
4.Quando la decisione non è impugnata ai sensi dell'articolo 35-*bis* del decreto legislativo 28 gennaio 2008 n.25 i dati relativi alle videoregistrazioni e ai verbali delle trascrizioni sono conservati per tre anni, ossia nel termine minimo previsto dall'art. 14, comma 3, del decreto legislativo 28 gennaio 2008, n.25 e alla scadenza sono eliminati definitivamente.
5. Quando è presentata impugnazione ai sensi dell'articolo 35-bis del decreto legislativo n.25 del 2008 i dati di cui al comma 4 sono conservati fino alla decisione definitiva, esclusivamente allo scopo di consentire le attività previste dal presente decreto.

ART. 6

(Clausola di invarianza finanziaria)

Le amministrazioni interessate provvedono all'attuazione delle disposizioni di cui al presente decreto nei limiti delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e comunque senza nuovi o maggiori oneri a carico della finanza pubblica.

ART. 7

(Disposizioni finali)

Il presente decreto è pubblicato sul Portale dei servizi telematici del Ministero della giustizia e sul sito internet del Ministero dell'interno e si applica ai procedimenti di cui all'articolo 35-bis del decreto legislativo n.25 del 2008 introdotti con ricorso depositato a partire dal 24 giugno 2025.

Roma lì_____

Il Capo Dipartimento
Innovazione Tecnologica
Ettore Sala

Ettore Sala

Il Presidente
Commissione Nazionale Asilo
Fabrizio Gallo

(documento firmato digitalmente)

Firmato Digitalmente da/Signed by:
FABRIZIO GALLO

In Data/On Date:
giovedì 12 dicembre 2024 09:56:11

Ministero della Giustizia

Ministero dell'Interno

SPECIFICHE TECNICHE PER LA MESSA A DISPOSIZIONE DEL GIUDICE E DELL'AVVOCATO DELLA VIDEOREGISTRAZIONE DEL COLLOQUIO DEL RICHIEDENTE ASILO

AMBITO DI APPLICAZIONE

Il presente documento contiene le specifiche tecniche relative all'iscrizione al servizio e alla relativa fruizione dei contenuti, in particolare delle videoregistrazioni del colloquio dei richiedenti asilo.

Le presenti specifiche regolamentano:

- l'accesso alle funzionalità di standard dell'applicazione S.IN.D.A.C.A., nonché all'area riservata nella quale è possibile eseguire i trattamenti del patrimonio informativo secondo almeno due profili autorizzativi associati a utenti finali distinti come di seguito indicati:
    i. accesso riservato ai magistrati;
    ii. accesso riservato agli avvocati.

Le informazioni essenziali per identificazione del personale (Gestione delle Identità) da abilitare agli accessi sono:

- i dati identificativi del magistrato;
- i dati identificativi e l'indirizzo di posta elettronica certificata dell'avvocato;
- l'ordine professionale di appartenenza dell'avvocato;
- i dati identificativi delle informazioni oggetto della richiesta (Codice CUI).

Nello specifico, il presente documento descrive la gestione delle richieste di autorizzazione degli accessi mediante web Services al patrimonio di S.IN.D.A.C.A.:

- le modalità di inserimento telematica della prima e delle successive richieste di autorizzazione al CUI;
- le modalità di controllo automatico della completezza e correttezza della richiesta di autorizzazione;
- le modalità di validazione della richiesta di autorizzazione;
- le modalità di revisione delle richieste di autorizzazione;
- le modalità di sospensione o revoca delle richieste di autorizzazione.

Inoltre, saranno identificate e descritte le caratteristiche specifiche dei profili autorizzativi ammessi alla consultazione dei dati delle registrazioni audio-video.

DEFINIZIONI

ADDETTI UPP: le persone assegnate all'ufficio per il processo costituito presso il Tribunale in cui hanno sedi le sezioni specializzate dei Tribunali ordinari che si occupano di immigrazione, protezione internazionale e libera circolazione dei cittadini dell'Unione europea istituita ai sensi dell'articolo 1, decreto-legge 17 febbraio 2017, n.13 (convertito, con modificazioni, con legge 13 aprile 2017. n.46);

ARCHIVIAZIONE: processo di memorizzazione sistematica della registrazione audio-video dell'audizione del richiedente asilo all'interno di uno spazio digitale tale (storage) che tali elementi rimangano presenti e integri in modo ordinato e non casuale per poter essere facilmente accessibili ed utilizzabili per un uso futuro. All'interno dello storage di S.IN.D.A.C.A. tali requisiti di integrità e disponibilità sono garantiti da software dedicato (attualmente HCP);

ASR CLIENT: applicazione installata sulle postazioni di lavoro periferiche del sistema S.IN.D.A.C.A. collocate presso le Commissioni e le sezioni territoriali per il riconoscimento della protezione internazionale che inviano i frame audio-video dell'audizione e riceve la relativa trascrizione effettuata dal server centrale ove è installato il motore ASR;

ASR SERVER: applicazione installata sul server centrale del sistema S.IN.D.A.C.A. che riceve i frame audio video dai Client collocati consente il colloquio con il server centrale ove è installato;

CAD: Codice per l'Amministrazione Digitale è il testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese, adottato con decreto legislativo 7 marzo 2005 n. 82;

CANCELLERIA: la cancelleria della sezione specializzata dei Tribunali ordinari che si occupano di immigrazione, protezione internazionale e libera circolazione dei cittadini dell'Unione europea istituita ai sensi dell'articolo 1, decreto-legge 17 febbraio 2017, n.13 (convertito, con modificazioni, con legge 13 aprile 2017. n.46);

CED: il Centro Elaborazione Dati del Dipartimento per le Libertà Civili e l'Immigrazione del Ministero dell'Interno;

Codice CUI: il codice univoco identità assegnato in fase di riconoscimento del cittadino di paese terzo o apolide assegnato dal sistema AFIS;

COMMISSIONE NAZIONALE: COMMISSIONE NAZIONALE PER IL DIRITTO D'ASILO: costituisce l'Autorità di riferimento del sistema italiano di protezione internazionale, dotata di compiti di indirizzo e coordinamento delle Commissioni e delle Sezioni territoriali per il riconoscimento della protezione internazionale. Ha inoltre competenze decisionali in materia di eventuale revoca e cessazione delle forme di protezione già riconosciute dai suddetti organismi, di seguito Commissione Nazionale;

COLLEGI TERRITORIALI: COMMISSIONI E SEZIONI TERRITORIALI PER IL RICONOSCIMENTO DELLA PROTEZIONE INTERNAZIONALE: articolazioni territoriali del Sistema Asilo che si occupano con poteri decisionali delle domande di riconoscimento della protezione internazionale, di seguito Collegi territoriali;

DLCI-MINISTERO DELL'INTERNO-: il Dipartimento per le Libertà Civili e l'Immigrazione del Ministero dell'Interno, articolazione del Ministero dell'Interno presso cui risultano incardinate la Commissione Nazionale per il Diritto di asilo e l'Ufficio II- Ufficio informatico;

HCP: (*Hitachi Content Platform*) soluzione tecnologica che viene attualmente utilizzata nello storage S.IN.D.A.C.A. per assicurare il rispetto dei criteri di archiviazione richiesti dalla normativa in vigore;

HTTPS: *(HyperText Transfer Protocol over Securesocketlayer)* indica il protocollo di accesso alle informazioni fruibili sul World Wide WEB. La lettera S indica la versione del protocollo http che utilizza un canale di trasporto cifrato per esempio SSL(SecureSocketLayer) o Transport Security Layer(TLS);

IPT: *(Information Technology)* Tecnologie riguardanti i sistemi, le apparecchiature, i server e i sistemi interconnessi di apparecchiature utilizzati per l'acquisizione, l'archiviazione, l'elaborazione, la gestione, il controllo, la visualizzazione di dati o informazioni;

ICT: ***(****Information e Communication Technology)* Tecnologie riguardanti le apparecchiature, i server e i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare dati e informazioni;

LAN: *(Local Area Network)* rete informatica estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come una porzione di edificio, un edificio o un complesso di edifici adiacenti;

MOTORE ASR: *(Automatic Speech Recognition)* applicazione basata su tecnologia Client/Server che consente il riconoscimento automatico del parlato naturale della lingua italiana, l'indicizzazione dei singoli frame audio-video e la relativa trascrizione;

PCT: il processo civile telematico come regolato dal decreto del Ministro della Giustizia 31 marzo 2011, n.44;

ReGIndE: il registro generale degli indirizzi elettronici, come definito all'art. 7 del Regolamento DM 21 febbraio 2011, n.44;

RETE INTRANET: rete privata dedicata alla interconnessione delle amministrazioni e degli enti pubblici nazionali;

SAML: *(Security Assertion Markup Language)* standard di federazione aperto che consente una comunicazione sicura tra più domini e tra il cloud pubblico e altri sistemi abilitati trasferendo il Token di autenticazione a un'altra applicazione, e che svolge due principali funzioni di sicurezza: 1) l'autenticazione che consiste nella conferma dell'identità degli utenti; 2) l'autorizzazione che è un passaggio dell'autorizzazione utente alle applicazioni per l'accesso a determinati sistemi o contenuti;

SERVER: dispositivo o sistema informatico connesso in rete, pubblica o privata, che consente di utilizzare le risorse condivise dallo stesso (dati, programmi, hardware), da parte di ulteriori dispositivi o sistemi informati chiamati client che si connettono alla rete;

SPC- Sistema Pubblico di Connettività: ~~i~~nsieme di regole tecniche e di principi che definisce le modalità preferenziali che i sistemi informativi delle pubbliche amministrazioni devono adottare per essere tra loro interoperabili. È la cornice nazionale di interoperabilità;

SEZIONE SPECIALIZZATA: la sezione specializzata dei Tribunali ordinari in materia di immigrazione, protezione internazionale e libera circolazione dei cittadini dell'Unione europea istituita ai sensi dell'articolo 1, decreto-legge 17 febbraio 2017, n.13 (convertito, con modificazioni, con legge 13 aprile 2017, n.46);

S.IN.D.A.C.A.*(Sistema Informativo di documentazione delle Audizione delle Commissioni Asilo)*: il sistema informatico utilizzato per la videoregistrazione delle audizioni dei richiedenti protezione internazionale e per la trascrizione della relativa verbalizzazione, mediante riconoscimento automatico del parlato;

SLA (*Service Level Agreement):* sono i livelli di servizio che vengono garantiti in termini di accessibilità e disponibilità del servizio IT;

TECNOLOGIA BLADE SERVER: dispositivo hardware pensato per minimizzare l'occupazione di spazio. I server Blade tipicamente un server (fisico) distinto che singolarmente o in concorso con altre lame, può simulare N macchine server virtuali;

TECNOLOGIA STORAGE: si identificano i dispositivi hardware, i supporti per la memorizzazione, le infrastrutture ed i software dedicati alla memorizzazione non volatile di grandi quantità di informazioni in formato elettronico;

TLS:*(Transport Security Layer)* protocollo crittografico che permette una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti, come ad esempio Internet, fornendo autenticazione, integrità dei dati e confidenzialità;

TOKEN: struttura dati funzionale alla fase di accreditamento dei soggetti autorizzati ad accedere con le diverse modalità previste ai file archiviati nel sistema S.IN.D.A.C.A.;

URL: *Uniform Resource Locator* è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete pubblica o privata;

VESTA.NET *(Verifica Status)*: applicazione web pubblicata sulle reti intranet, dedicate alla gestione delle istanze di protezione internazionale, ad uso esclusivo degli utenti delle Commissioni Territoriali per il riconoscimento della protezione internazionale e relative Sezioni e della Commissione Nazionale per il Diritto di Asilo;

WEB SERVICE: Servizi Web fruibili sia in modalità Client To Server sia in modalità Server To Server. I servizi possono essere erogati tramite specifici web server o application server mediante l'utilizzo di protocolli HTTPS;

XSD: file scritto nel linguaggio dello schema XML, utilizzato per definire quali elementi e attributi possono apparire in un documento XML che definisce anche la relazione degli elementi e quali dati possono essere memorizzati in essi;

XML: *(eXtensible Markup Language)* metalinguaggio basato su un meccanismo sintattico di marcatori (markup), fatto da una serie di istruzioni (tag), che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo e permette di creare documenti e dati strutturati in formato elettronico.

INFRASTRUTTURE TECNOLOGICHE INFORMATICHE E DI RETE

Le infrastrutture IT e la rete Intranet SPC di interconnessione dei CED del Ministero di giustizia e dei CED del Ministero dell'interno di competenza del DLCI garantiscono la gestione di tutti gli aspetti tecnologici, funzionali e non funzionali. In particolare, sono garantiti l'erogazione dei servizi applicativi, dei servizi web e dei servizi di accoglienza mediante portali WEB specifici.
Sono previste specifiche tecniche funzionali a garantire la disponibilità dei servizi e dei micro-servizi IT, delle componenti applicative dei servizi WEB (per es.: portali WEB) e dei servizi di archiviazione dei dati.
L'architettura generale dei servizi IT erogati prevede il disaccoppiamento dei servizi di:

- Accoglienza posizionati su sistemi ad accesso selettivo localizzati sul punto di accesso Intranet SPC (Accesso soggetti di cui all'articolo 4, comma 1 lett. b) e c) del decreto direttoriale);
- Presentazione dei dati mediante front-end e, localizzato sul punto di accesso da Intranet SPC (Accesso soggetti di cui all'articolo 4, comma 1 lett. b) e c) del decreto direttoriale);
- Presentazione dei dati mediante front-end esposto su Internet, localizzato sul punto di accesso di Internet (Accesso soggetti di cui all'articolo 4, comma 1 lett. a) del decreto direttoriale);
- Archiviazione dati sui sistemi posizionati in back-end, non raggiungibili direttamente dall'esterno del CED.

I punti di accesso realizzano autonomamente la parte di front-end, e sono raggiungibili da reti distinte:

- Rete SPC Intranet per gli accessi dei magistrati;
- Rete Internet per gli accessi degli avvocati.

I sistemi di archiviazione non sono accessibili direttamente agli utenti dall'esterno del CED dalla rete internet o dalla Rete SPC.
L'accesso ai servizi di consultazione avviene esclusivamente mediante canale di trasporto sicuro (protocollo TLS) previa identificazione digitale sui punti di accesso specifici.

DESCRIZIONE DELLE FUNZIONALITA'

Nella fase di iscrizione ed accreditamento alla fruizione dei servizi previsti per i soggetti di cui all'art. 4 comma 4 del decreto direttoriale devono essere indicate una serie di informazioni essenziali contenute nel Token inviato dai sistemi del Ministero della giustizia (Userid) tali da consentire l'identificazione digitale dell'utente e l'associazione al suo profilo autorizzativo secondo le modalità specificate nel presente documento. Successivamente all'accreditamento sarà dunque eseguita l'identificazione dei soggetti accreditati tramite associazione dei dati contenuti nel Token (Userid) alla specifica identità digitale.

L'utente con il profilo "Magistrato, Cancelliere della Sezione specializzata, Addetto al UPP" (soggetti di cui all'articolo 4, comma 1 lett. b) e c) del decreto direttoriale) sarà automaticamente autenticato dai sistemi di giustizia e potrà accedere direttamente all'applicazione che eroga i contenuti delle videoregistrazioni del colloquio (S.IN.D.A.C.A.).

L'utente con il profilo "Avvocato" (soggetti di cui all'articolo 4, comma 1, lett. a) del decreto direttoriale) sarà autenticato tramite la propria identità digitale secondo le modalità previste dal CAD e successivamente specificate.

Le autorizzazioni concesse saranno adeguate, in termini di pertinenza e non eccedenza, ai trattamenti che saranno eseguiti dalle diverse tipologie di utenze e in linea con le funzionalità disponibili sull'applicazione che eroga il servizio dei contenuti delle videoregistrazioni, secondo le specifiche dettagliate nei successivi paragrafi.

Le funzionalità essenziali che saranno erogate del servizio di accoglienza dell'applicazione S.IN.D.A.C.A. sono quelle di **s**eguito elencate:

- Ricerca: secondo i criteri di selezione idonei all'identificazione univoca della ricerca indicando gli oggetti della ricerca (es. Identificativo CUI), Data Ricerca, Stato degli oggetti della ricerca (es. Attivo, In corso di abilitazione, Disabilitato);
- Visualizzazione Ricerca: esito della ricerca e risultato della ricerca;
- Fruizione dei contenuti secondo i privilegi associati ai profili autorizzativi specifici previsti per i soggetti di cui all'articolo 4, comma 6 del decreto direttoriale.

Qualora venga eseguita una ricerca su un CUI non presente sull'applicazione S.IN.D.A.C.A. l'esito della ricerca risulterà negativo e il sistema restituirà l'informazione che il CUI oggetto di ricerca non è presente.

DESCRIZIONE REQUISITI DI SICUREZZA

I requisiti di sicurezza previsti sia per i protocolli comunicazioni tra i sistemi IT del Ministero della Giustizia e del Ministero dell'Interno sia per l'applicazione S.IN.D.A.C.A. sono stati definiti al fine di garantire la sicurezza delle informazioni stesse dalla perdita di riservatezza, integrità e disponibilità.
L'applicazione S.IN.D.A.C.A. al fine di garantire i requisiti di sicurezza di Integrità dispone di soluzioni tecnologiche che garantiscono il principio di immodificabilità di tutti i file audio e video, verbali ed altri documenti archiviati. La soluzione tecnologica attualmente utilizzata è HCP.
L'applicazione S.IN.D.A.C.A. al fine di garantire i requisiti di sicurezza di disponibilità della sua architettura IT e Storage dispone di soluzione tecnologiche che garantiscono l'alta affidabilità e di conseguenza l'erogazione del servizio secondo gli SLA preventivamente concordati tra le parti per la consultazione di tutti i file: Audio e Video e Verbali archiviati su S.IN.D.A.C.A..
Al fine di assicurare i requisiti di riservatezza che le informazioni siano accessibili solo alle persone autorizzate è stato previsto che gli utenti siano identificati in modo univoco mediante l'utilizzo di strumenti idonei:

- tramite federazione con sistemi giustizia per le utenze relative ai soggetti di cui all'articolo 4, comma 1 lett. b) e c) del decreto direttoriale, con identificazione a cura del Ministero della giustizia al momento dell'accesso di tali profili ai propri sistemi;
- con modalità previste dal CAD per l'accesso soggetti di cui all'articolo 4, comma 1 lett. a) del decreto direttoriale, con identificazione effettuata a cura del Ministero dell'interno.

ACCREDITAMENTO E VALIDAZIONE DEI SOGGETTI ABILITATI

La responsabilità del processo di validazione dell'abilitazione degli accessi per i soggetti di cui all'art. 4 comma 1 del Decreto direttoriale è in carico al Ministero della giustizia e la richiesta di autorizzazione all'accesso al patrimonio dell'applicazione S.IN.D.A.C.A. dovrà contenere le informazioni minime obbligatorie per l'accesso medesimo.

La trasmissione delle richieste di autorizzazione avverrà su Rete Privata Intranet SPC mediante l'ausilio di protocolli di trasporto sicuri, protocollo TLS in versione 1.2 o superiori, oppure

mediante la realizzazione di una Virtual Private Network (VPN) tra la rete del Ministero della Giustizia e la rete dei Data Center del DLCI del Ministero dell'interno.

L'applicazione S.IN.D.A.C.A. acquisita la richiesta, consente l'accesso, a fronte della corrispondenza delle informazioni oggetto del Servizio automatizzato di scambio, associando alle anagrafiche presenti nelle richieste gli specifici profili autorizzativi secondo i profili e ruoli nella quale sono identificati gli specifici trattamenti. I ruoli attualmente definiti sono quello relativo ai privilegi di lettura/consultazione, esclusivamente sull'archivio SINDACA da parte dei soggetti di cui all'articolo 4, comma 1 lettere b) e c) del decreto direttoriale, e quello relativo alla richiesta di trasferimento dati in download, per il profilo Avvocato (soggetti di cui all'articolo 4, comma1 lettera a) del decreto direttoriale, che accederà ad un repository distinto dall'archivio SINDACA nel quale verranno posizionati i dati della videoregistrazione.

ACCESSO DEI SOGGETTI ABILITATI

MODALITÀ DI ACCESSO E FRUIZIONE DEI CONTENUTI DA PARTE DEI SOGGETTI DI CUI ALL'ARTICOLO 4, COMMA 1 LETTERE B) E C) DEL DECRETO DIRETTORIALE

L'utente al quale è stato associato il profilo autorizzativo (soggetti di cui all'articolo 4, comma 1 lettere b) e c) del decreto direttoriale) accede all'applicazione S.IN.D.A.C.A. tramite rete di interconnessione Intranet Servizio Pubblico di Connettività (SPC)**,** mediante una URL pubblicata dal Ministero della Giustizia sulla rete Intranet SPC.

Il Ministero della giustizia ha reso disponibile un sistema di autenticazione in modalità federata che permette tramite protocollo SAML 2.0 di eseguire l'autenticazione del Magistrato all'applicazione S.IN.D.A.C.A.. Nell'asserzione SAML 2.0 inviata a S.IN.D.A.C.A., avviene mediante protocolli di trasporto TLS V 1.2 o superiori, a seguito dell'autenticazione saranno trasmessi i parametri, relativi ai dati anagrafici, indicati come obbligatori nella richiesta di autorizzazione di accesso (Denominato "Token" di richiesta autorizzazione), a S.IN.D.A.C.A..
Si riportano di seguito i parametri obbligatori: username, codice fiscale, qualifica. Tali dati sono essenziali ad individuare in modo univoco l'utente al quale associare su S.IN.D.A.C.A. un profilo autorizzativo specifico a garantire il "Need to Know".
In fase di avvio in produzione del sistema si valuterà l'opportunità di inserire ulteriori dati quali, ad esempio: profilo autorizzativo, data di abilitazione della username, procedimento di riferimento.

L'applicazione S.IN.D.A.C.A. consentirà l'accesso ai contenuti solo dopo avere verificato l'effettiva corrispondenza tra le informazioni afferenti all'utente che intende accedere e i parametri obbligatori pervenuti dal Ministero della giustizia presenti nel "Token" di autorizzazione; in particolare verifica l'esistenza dei CUI associati al Codice Fiscale e all'account ricevuto mediante il Servizio automatizzato di scambio di informazioni tra DLCI del Ministero dell'interno ed il Ministero della giustizia. Qualora la verifica automatica eseguita abbia esito positivo l'utente con profilo di cui all'art. 4. comma 1 lett. b) e c) del Decreto direttoriale sarà abilitato alla funzionalità di ricerca per l'accesso ai trattamenti sui CUI che sono presenti e disponibili sull'applicazione S.IN.D.A.C.A..

L'applicazione S.IN.D.A.C.A. consentirà una singola connessione per i soggetti di cui all'articolo 4, comma 1 lettere b) e c) del decreto direttoriale e verificherà costantemente il numero di utenti connessi contemporaneamente al fine di garantire un livello di disponibilità del servizio adeguato alla fruizione senza interruzioni del servizio video e audio. Nel caso sia superato il numero massimo di connessione concorrenti sarà restituito all'utente messaggio di indisponibilità temporanea del servizio.

Il profilo autorizzativo relativo ai soggetti di cui all'articolo 4, comma 1 lettere b) e c) del decreto direttoriale è realizzato al fine di garantire il principio del "Least Privilege"; in particolare è consentito esclusivamente il trattamento in visualizzazione dei contenuti video e audio.

Inoltre, tale profilo autorizzativo è stato realizzato per garantire la riservatezza dei trattamenti dati ed il principio di pertinenza e non eccedenza dei trattamenti dati, in quanto è possibile visualizzare solo i dati relativi al CUI di competenza riconducibile al procedimento indicato nella richiesta di autorizzazione accesso.

MODALITÀ DI ACCESSO E FRUIZIONE DEI CONTENUTI DA PARTE DEI SOGGETTI DI CUI ALL'ARTICOLO 4, COMMA 1 LETTERA A) DEL DECRETO DIRETTORIALE

Il profilo autorizzativo associato all'utenza definita per i soggetti di cui all'art. 4 comma 1, lett. a) del decreto direttoriale, Avvocato, è stato realizzato per garantire la riservatezza del trattamento in download dei file audio e video al fine di garantire il principio di pertinenza e

non eccedenza dei trattamenti dati: l'utente con profilo Avvocato potrà scaricare solo i dati relativi ai CUI a cui è abilitato che sono quelli riconducili al procedimento indicato nella richiesta di autorizzazione (denominato anche "Token" di autorizzazione o Userid).

L'utente-avvocato, previa validazione dell'abilitazione all'accesso da parte dell'ufficio giudiziario cui appartengono le sezioni specializzate, potrà effettuare la richiesta (prenotazione) di download dei contenuti tramite una URL specifica, pubblicata dal Ministero dell'Interno, indicando il/i CUI di interesse. L'applicazione S.IN.D.A.C.A. verifica la completezza delle informazioni obbligatorie e la congruenza delle informazioni presenti nel "Token" di autorizzazione (Userid); cioè verifica l'esistenza dei CUI associati al Codice Fiscale e all'account di PEC dell'utente-avvocato ricevuto mediante il servizio automatizzato di scambio di informazioni tra il DLCI del Ministero dell'interno e l'ufficio giudiziario cui appartengono le sezioni specializzate.
Una volta effettuata – tramite URL - la selezione del CUI per il quale è autorizzato al trattamento, riceverà una mail al suo indirizzo di PEC contenente il link dove poter fare il download del file criptato contenente la registrazione audio-video dell'audizione richiesta.
Raggiunto il link per effettuare il download del file, l'utente dovrà nuovamente autenticarsi tramite la propria identità digitale.

Solo dopo il completamento del download dei file criptati sarà inviata all'indirizzo PEC dell'utente-avvocato la password che consentirà l'apertura dei file criptati precedentemente scaricati.
Con l'adozione di questa soluzione l'Avvocato disporrà di un profilo autorizzativo per trattare i dati secondo i principi del "Need To Know" e del "Least Privilege" in modo da garantire un livello di riservatezza elevato e adeguato ai contenuti presenti nei file trasferiti al fine di prevenire ed evitare trattamenti illeciti o non autorizzati di terze parti.

È previsto che l'accesso tramite link ai file sarà reso possibile per un tempo determinato, fissato in 15 giorni solari. Nel caso l'utente debba accedere ai file oltre il termine predeterminato per la loro fruizione, questo dovrà ripetere la procedura di prenotazione.

AGGIORNAMENTO DEI DATI

Le modalità di aggiornamento dei dati anagrafici sono eseguite sia per la prima richiesta di autorizzazione sia per le successive richieste. Le attività di aggiornamento saranno eseguite mediante un servizio automatizzato di trasferimento di informazioni con collegamento unidirezionale dalle CANCELLERIE verso il DLCI - Ministero dell'Interno, utilizzando la connettività di rete Intranet SPC su canale di trasporto sicuro mediante protocollo TLS. L'applicazione S.IN.D.A.C.A., sarà invocata mediante servizi web in modalità asincrona tramite l'ausilio di API REST che scambiano dati in formato JavaScript Object Notation (JSON).

L'applicazione S.IN.D.A.C.A. acquisisce i flussi delle informazioni inviate dai servizi IT sorgenti del Ministero della giustizia e verifica la completa compilazione delle informazioni classificate obbligatorie.

Le informazioni obbligatorie per i rispettivi utenti e profili, risultano le seguenti:

- Anagrafica giudice: Nome e Cognome e Codice fiscale;
- Anagrafica CUI associazione singolo giudice: Identificativo/i CUI fruibile all'utente e Stato del/i CUI (es. Associato o Cancellato);
- Anagrafica avvocato: nome e cognome, codice fiscale, indirizzo di Posta elettronica Certificata (PEC);
- Anagrafica CUI associazione singolo avvocato: Identificativo/i CUI fruibile all'utente e Stato del/i CUI (es. Associato o Cancellato);
- Anagrafica CUI associazione Multipla: Identificativo/i CUI fruibile/i a diversi Giudici ed Avvocati e Stato del/i CUI (es. Associato o Cancellato).

ARCHIVIAZIONE DEI DATI

I principi di archiviazione sono correlati alle tipologie di dati ed ai principi di necessità e finalità del trattamento, secondo i quali i dati raccolti non possono essere trattati per un tempo ulteriore rispetto a quello strettamente necessario allo scopo della raccolta.

I dati soggetti ad archiviazione on-line sono i seguenti:

a) dati, in formato non compresso e accessibili direttamente dallo storage dell'applicazione S.IN.D.A.C.A., relativi alla video registrazione dell'audizione;
b) dati, in formato non compresso e accessibili direttamente da un'area costituita ad hoc ed esterna allo storage dell'applicazione S.IN.D.A.C.A., relativi ai dati contenuti nel Token del sistema di autenticazione.

Il processo di archiviazione dei dati On-line è funzionale all'erogazione del servizio secondo gli SLA Concordati.
I dati relativi alle videoregistrazioni e ai verbali delle trascrizioni sono conservati nel rispetto del termine previsto dall'art. 14, comma 3, del decreto legislativo del 28/01/2008 n.25 e alla scadenza di tale termine sono eliminati definitivamente, salvo quanto previsto dal comma 5 dell'art. 5 del presente decreto.
In caso di rigetto della domanda di protezione internazionale e di impugnazione ai sensi dell'articolo 35 bis del predetto decreto legislativo, i dati sono conservati fino alla decisione definita esclusivamente allo scopo di consentire lo svolgimento delle attività previste dal presente decreto.

I dati delle videoregistrazioni delle audizioni sono protetti da apposita piattaforma software (attualmente HCP) che ne garantisce la non sostituibilità, la non manomissione e non cancellazione per tutto il periodo previsto. Tali dati sono accessibili solo agli utenti dei Collegi territoriali limitatamente alle audizioni personalmente svolte e ai soggetti di cui all'art. 4, comma 1 del Decreto direttoriale.

I dati relativi ai Token del processo autorizzativo (Userid) sono trattati tutti in maniera automatica e non leggibili da funzioni esterne ad eccezione dei dati di log nel caso dovessero essere svolti accertamenti di sicurezza in funzione di accessi anomali o abnormi.

Il Capo Dipartimento
Innovazione Tecnologica
Ettore Sala

Ettore Sala

Il Presidente
Commissione Nazionale Asilo
Fabrizio Gallo

Documento firmato digitalmente

Firmato Digitalmente da/Signed by:
FABRIZIO GALLO

In Data/On Date:
giovedì 12 dicembre 2024 09:57:41