



Ministero delle infrastrutture e della mobilità sostenibili

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

Regole tecniche concernenti il trattamento dei dati personali effettuato dal Ministero delle infrastrutture e della mobilità sostenibili attraverso i sistemi di *Face Recognition* utilizzati nell'ambito dello svolgimento degli esami di teoria per conseguire le patenti di guida di cui all'articolo 116 commi 3, 4 e 11 del D.Lgs. 30 aprile 1992, n. 285, recante «Nuovo codice della strada»

Visto il D.Lgs. 30 luglio 1999, n. 300, recante «*Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59*»;

Visto il D.Lgs. 30 marzo 2001, n. 165, recante «*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*», con particolare riferimento agli articoli 16 e 17 con i quali sono state disciplinate, rispettivamente, le «*Funzioni di dirigenti di uffici dirigenziali generali*» e di «*Funzioni di dirigenti*»;

Visto il D.P.C.M. 23 dicembre 2020, n. 190 di riorganizzazione del Ministero delle infrastrutture e dei trasporti (a seguire, anche «MIMS» o «Ministero»), come da D.L. 1° marzo 2021, n. 22, convertito con modificazioni dalla Legge 22 aprile 2021, n. 55;

Visto, in particolare, l'articolo 18, comma 1 del citato D.P.C.M. n. 190/2020, il quale prevede che «*fino all'adozione del decreto di cui all'articolo 16, comma 3, ciascun ufficio di livello dirigenziale generale opera avvalendosi dei preesistenti uffici dirigenziali di livello non generale con le competenze nel rispettivo settore di attribuzione*»;

Visto il Decreto del MIMS del 30 novembre 2021 n. 481, registrato dalla Corte dei Conti il 19 dicembre 2021 con il n. 3089, con cui sono stati rimodulati ed individuati il numero ed i compiti degli uffici dirigenziali di livello non generale del Ministero, di cui all'articolo 16, comma 3 del citato decreto del Presidente del Consiglio dei ministri 23 dicembre 2020, n. 190;

Vista la Legge 30 dicembre 2021, n. 234, recante il «*Bilancio di previsione dello Stato per l'anno finanziario 2022 e il bilancio pluriennale per il triennio 2022-2024*»;

Visto il Decreto del Ministero dell'Economia e delle Finanze del 31 dicembre 2021, recante la «*Ripartizione in capitoli delle Unità di voto parlamentare relative al bilancio di previsione dello Stato per l'anno finanziario 2022 e per il triennio 2022-2024*»;

Vista la Direttiva del MIMS, prot. n. 3 del 10 gennaio 2022, per l'attività amministrativa e la gestione, con la quale sono stati conferiti ai titolari dei centri di responsabilità amministrativa gli obiettivi strategici ed operativi per l'anno 2022 ed assegnate le risorse finanziarie, umane e strumentali di competenza;

Vista la Direttiva n. 3 del 20 gennaio 2022, con la quale sono state assegnate ai titolari delle Direzioni Generali e delle Direzioni Generali Territoriali gli obiettivi e le risorse per l'anno 2022;

Vista la Direttiva n. 12 del 26 gennaio 2022, con la quale sono stati assegnati per l'anno 2022 gli obiettivi e le relative risorse finanziarie ai direttori delle Divisioni della Direzione Generale per la Motorizzazione, per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione;

Visto il D.P.C.M. 11 giugno 2021 concernente il Decreto di incarico di funzione dirigenziale di livello generale conferito ai sensi dell'articolo 19, comma 4 del D.Lgs. n. 165/2001 all'Ing. Pasquale D'Anzi, nominato



Ministero delle infrastrutture e della mobilità sostenibili

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

Direttore generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione, ammesso alla registrazione della Corte dei Conti il 6 luglio 2021 al n. 2229;

Vista la Direttiva 2006/126/CE del Parlamento europeo e del Consiglio, del 20 dicembre 2006, concernente la patente di guida, che definisce, tra l'altro, il modello di patente di guida attualmente utilizzato in ambito comunitario, le modalità di riconoscimento reciproco, le misure di antifalsificazione, le categorie di patenti e le età minime per il conseguimento delle stesse, nonché le modalità di rilascio, validità e rinnovo;

Vista la Direttiva 2009/113/CE della Commissione, del 25 agosto 2009, recante «*Modifica della direttiva 2006/126/CE concernente la patente di guida*»;

Visto il D.Lgs. 30 aprile 1992, n. 285, recante «*Nuovo codice della strada*», e successive modificazioni (di seguito, anche «*Codice della Strada*»);

Visto, in particolare, l'art. 116 del Codice della Strada, recante «*Patente e abilitazioni professionali per la guida di veicoli a motore*», che specifica le differenti categorie di patenti di guida, elencandone i requisiti minimi di conseguimento ed eventuali limitazioni;

Visto, in particolare, l'art. 121 del Codice della Strada, recante «*Esame di idoneità*», che, tra l'altro, prevede che l'idoneità tecnica per il rilascio di una patente di guida si consegue superando una prova di controllo delle cognizioni ed una prova di verifica delle capacità e dei comportamenti e che i predetti esami sono effettuati secondo direttive, modalità e programmi stabiliti con decreto del MIMS sulla base delle direttive della Comunità europea;

Visto il decreto del Presidente della Repubblica 16 dicembre 1992, n. 495, recante «*Regolamento di esecuzione e di attuazione del nuovo codice della strada, e successive modificazioni*»;

Visto il decreto del Ministro dei trasporti e della navigazione 17 maggio 1995, n. 317, e successive modificazioni, concernente «*Regolamento recante la disciplina dell'attività delle autoscuole*»;

Visto il decreto del MIMS 30 settembre 2003, n. 40T, pubblicato nella Gazzetta Ufficiale, n. 88 del 15 aprile 2004, recante «*Disposizioni comunitarie in materia di patenti di guida e recepimento della direttiva 2000/56/CE. (Decreto n. 40T)*»;

Visto il decreto legislativo 18 aprile 2011, n. 59, recante «*Attuazione delle direttive 2006/126/CE e 2009/113/CE concernenti le patenti di guida*» e successive modificazioni;

Visto il Decreto del 10 dicembre 2012, pubblicato nella Gazzetta Ufficiale n. 9 dell'11 gennaio 2013, recante «*Disciplina della prova di controllo delle cognizioni e di verifica delle capacità e dei comportamenti per il conseguimento della patente di categoria AM, nonché delle modalità di esercitazione alla guida di veicoli per i quali è richiesta la predetta patente*»;

Visto il decreto del MIMS 19 dicembre 2012, pubblicato nella Gazzetta Ufficiale n. 25 del 30 gennaio 2013, recante «*Disciplina della prova di controllo delle cognizioni e di verifica delle capacità e dei comportamenti per il conseguimento della patente di categoria B1, B e BE*»;

Visto il decreto del MIMS 8 gennaio 2013, pubblicato nella Gazzetta Ufficiale n. 25 del 30 gennaio 2013, recante «*Disciplina della prova di controllo delle cognizioni e di verifica delle capacità e dei comportamenti per il conseguimento delle patenti di categoria A1, A2 e A*»;



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

Vista la circolare n. 28819 del 19 settembre 2019, recante «*Procedure amministrative per il conseguimento della patente di guida della categoria B*», che prevede l'obbligo per i candidati, che vogliono presentare istanza per richiedere la patente di guida, di presentare due foto recenti (non anteriori a 6 mesi), uguali, formato tessera su fondo bianco e a capo scoperto (per motivi religiosi è consentito al candidato presentare fotografie con il campo coperto a condizione che i tratti del volto siano ben riconoscibili), stampate su carta di alta qualità e risoluzione;

Vista la circolare n. 28822 del 19 settembre 2019, recante «*Procedure amministrative per il conseguimento della patente di guida delle categorie A1, A2 e A*», che prevede il medesimo obbligo di cui alla circolare n. 28819 del 19 settembre 2019 esplicitato nel precedente punto;

Visto il decreto del 27 ottobre 2021 del MIMS, recante «*Modifiche alle modalità di espletamento della prova di verifica delle cognizioni per il conseguimento delle patenti di categoria A1, A2, A, e di categoria B1, B e BE*» finalizzato a conformare le modalità di esame di cui all'art. 1, comma 2, del citato decreto ministeriale 8 gennaio 2013, per le patenti di categoria A1, A2 ed A e del citato decreto ministeriale 19 dicembre 2012, per le patenti di categoria B1, B e BE;

Visto il 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 (a seguire, anche «GDPR»);

Visto, in particolare, l'articolo 6, paragrafo 1, lettera e) del GDPR, che consente il trattamento dei dati quando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri di cui è investito il Titolare del trattamento;

Visto il medesimo articolo 6, paragrafo 3, lettera b) del GDPR, che stabilisce che la base giuridica su cui si fonda il trattamento dei dati effettuato per l'esecuzione di un compito di interesse pubblico sia stabilita dal diritto dello Stato membro e contenga disposizioni specifiche per adeguarsi alle disposizioni del GDPR;

Visto, inoltre l'articolo 9 paragrafo 2, lettera g), del GDPR, che consente il trattamento di particolari categorie di dati personali, tra cui sono ricompresi i dati biometrici, nei casi in cui «*[...] il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*»;

Visto il D.Lgs. 30 giugno 2003, n. 196, recante il «*Codice in materia di protezione dei dati personali*»;

Visto, in particolare l'articolo 2-ter del D.Lgs. 30 giugno 2003 n. 196, introdotto dal D.Lgs. 10 agosto 2018, n. 101 di adeguamento alle disposizioni del GDPR, e modificato dal D.L. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla L. 3 dicembre 2021, n. 205;

Visto, in particolare, l'articolo 2-sexies del D.Lgs. 30 giugno 2003 n. 196, che consente il trattamento delle «particolari categorie di dati personali» necessari per motivi di interesse pubblico rilevante, qualora sia previsto da disposizioni di legge o di regolamento, o da atti amministrativi generali, che contengano elementi specifici sul trattamento di tali dati;

Visto il medesimo articolo 2-sexies del D.Lgs. 30 giugno 2003 n. 196, che considera «rilevante» l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie elencate nelle lettere da a) a dd) del medesimo comma;



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

Visto l'articolo 2-septies del D.Lgs. 30 giugno 2003 n. 196, ai sensi del quale «*in attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo*»;

Viste le «*Linee Guida in materia di riconoscimento biometrico e firma grafometrica*», che costituiscono l'Allegato A al Provvedimento n. 513 del 12 novembre 2014, del Garante per la protezione dei dati personali;

Considerata la necessità di introdurre specifiche misure finalizzate allo snellimento complessivo ed alla velocizzazione delle procedure degli esami per il conseguimento della patente, al fine di migliorare la generale *performance* del sistema e di renderla effettivamente coerente con le tempistiche previste dall'articolo 122 del Codice della Strada e con le risorse umane di cui dispongono gli uffici della Motorizzazione;

Considerata la necessità, nell'ambito degli obiettivi di cui al punto precedente, di attivare «*un nuovo modello operativo che, al fine di consentire ai candidati l'accesso all'aula di esame per il tramite di parametri biometrici, prevede l'esecuzione automatizzata, tramite software di riconoscimento facciale, dell'attività di identificazione degli stessi*», così come riportato anche nel citato decreto del 27 ottobre 2021 del MIMS;

Considerato che, a tal fine, sono stati sviluppati sistemi di *Face Recognition* idonei a semplificare e informatizzare le procedure di identificazione dei candidati che devono sostenere l'esame della patente di guida, eliminando i rischi connessi al riconoscimento *de visu*, nonché a evitare eventuali comportamenti contrastanti con la normativa vigente nonché lesivi degli interessi generali in materia di sicurezza e regolarità della circolazione stradale;

Considerato che i citati sistemi di *Face Recognition* saranno utilizzati sia ai fini dell'accesso dei candidati all'aula d'esame, che al fine di consentire l'accesso del candidato alla procedura di svolgimento dell'esame, nonché ai fini del riconoscimento del candidato per tutta la durata di svolgimento dell'esame;

Considerato che tali sistemi saranno resi operativi in tutte le aule del territorio nazionale previa sperimentazione;

Considerato che i sistemi che si intende utilizzare nell'ambito del suddetto modello operativo prevedono il trattamento di dati biometrici dei soggetti che devono svolgere l'esame di teoria per il conseguimento della patente di guida di cui all'articolo 116 commi 3, 4 e 11 del D.Lgs. 30 aprile 1992, n. 285, e che, ai sensi di legge, tale trattamento deve essere previsto da una apposita base giuridica che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

Tenuto conto che il Ministero ha predisposto e approvato il documento di valutazione di impatto svolta ai sensi dell'art. 35 del GDPR e delle «*Linee Guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679*», adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati il 4 aprile 2017, e successivamente emendate il 4 ottobre 2017;

Tenuto conto che con il presente provvedimento (a seguire, anche «Decreto») il MIMS provvede a definire, ai sensi dell'articolo 2-sexies del D.Lgs. del 30 giugno 2003, n. 196, la base giuridica del trattamento di dati personali riguardante l'utilizzo dei sistemi di *Face Recognition* ai fini dell'identificazione dei candidati che svolgono gli esami di teoria per conseguire le patenti di guida di cui all'articolo 116 commi 3, 4 e 11 del D.Lgs. 30 aprile 1992, n. 285;

Tenuto conto che, ai sensi di quanto previsto dal succitato articolo 2-sexies, il presente Decreto definisce:

- a) le finalità del trattamento di dati personali effettuato mediante i sistemi di *Face Recognition*;
- b) i dati personali oggetto di trattamento e le modalità di acquisizione degli stessi;



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

- c) le modalità di funzionamento dei sistemi di *Face Recognition*;
- d) il ruolo dei soggetti coinvolti a vario titolo nel trattamento;
- e) le garanzie e le misure di sicurezza adottate nel rispetto della normativa sulla protezione dei dati personali di cui al GDPR e al D.Lgs. 30 giugno 2003, n. 196, e delle regole tecniche del Sistema, nonché delle «*Linee Guida in materia di riconoscimento biometrico e firma grafometrica*» - Allegato A al Provvedimento n. 513 del 12 novembre 2014 del Garante per la protezione dei dati personali;
- f) i diritti e le garanzie per gli interessati.

Per tutto quanto sopra esposto,

DECRETA

Art. 1

(Valore delle premesse e degli allegati)

1. Le premesse costituiscono parte integrante e sostanziale del presente Decreto, da valere alla stregua di giuridica presupposizione.
2. L'Allegato tecnico «*Principali garanzie e misure di sicurezza*» costituisce parte integrante e sostanziale del presente Decreto.

Art. 2

(Definizioni)

1. Ai fini del presente decreto, si intende per:
 - a) **Sistemi di *Face Recognition***: i sistemi, distinti in «*Sistema di Accesso e Riconoscimento al Varco*» e «*Sistema di Accesso e Riconoscimento all'Esame*», che governano le procedure di riconoscimento dei candidati attraverso dispositivi dotati di una *Web-Cam* e di un *software* utili a consentire il riconoscimento facciale del candidato, rispettivamente al momento di accesso alla sede d'esame e al momento antecedente l'inizio della prova, nonché per tutta la durata di svolgimento della stessa;
 - b) **Sistema di Accesso e Riconoscimento al Varco o Sistema Varco**: il sistema che permette di effettuare il riconoscimento facciale del candidato al fine di consentirgli l'accesso all'aula d'esame. Il riconoscimento facciale viene effettuato da un dispositivo *tablet*, dotato di una *Web-Cam* integrata, che acquisisce l'immagine del volto del candidato al fine di trasformarla in un *Template Biometrico* da confrontare con i *Template Biometrici* di tutti i candidati prenotati alle sessioni di esame previste nella giornata;
 - c) **Sistema di Accesso e Riconoscimento all'Esame o Sistema Esame**: il sistema che permette di effettuare il riconoscimento facciale del candidato, prima dell'inizio dello svolgimento della prova d'esame e per tutta la durata della stessa, attraverso un dispositivo *Thin-Client* dotato di una *Web-Cam* che acquisisce l'immagine del volto del candidato, prima dell'inizio dello svolgimento della prova d'esame e per tutta la durata della stessa, al fine di trasformarla in un *Template Biometrico* da confrontare dapprima con i *Template Biometrici* di tutti i candidati prenotati alla specifica sessione di esame e poi con il solo *Template* corrispondente a quello del candidato;
 - d) **Sistema Informativo della Motorizzazione Civile o SIMOT**: la banca dati centralizzata della Direzione generale per la motorizzazione e per i servizi ai cittadini e alle imprese in materia di trasporti e navigazione (a seguire, anche «*Direzione*»), contenente, tra l'altro, le immagini fotografiche digitali di tutti coloro che presentano istanza di prenotazione al fine di sostenere l'esame



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

di teoria per il conseguimento della patente di guida; fotografie che saranno stampate sulla patente di guida una volta che il candidato abbia conseguito l'abilitazione alla guida;

- e) **Repository immagini o Repository:** archivio digitale istituito presso ciascun Ufficio provinciale della Motorizzazione in cui sono memorizzate in modalità temporanea le immagini fotografiche, reperite dal SIMOT, dei candidati prenotati alle sessioni di esame previste nella giornata, da cui i Sistemi di *Face Recognition* estraggono i *Template* Biometrici utili per effettuare il confronto biometrico;
- f) **Candidato o Interessato:** l'esaminando che sostiene la prova di teoria per il conseguimento della patente, i cui dati personali costituiscono oggetto di trattamento da parte dei Sistemi di *Face Recognition*;
- g) **Trattamento di Dati Personali o Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- h) **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- i) **Dati Biometrici:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- j) **Caratteristica Biometrica:** caratteristica biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei tratti biometrici distintivi e idonei al riconoscimento biometrico;
- k) **Campione Biometrico:** rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine del processo di acquisizione;
- l) **Template Biometrico** (a seguire, anche «*Template*»): insieme di tratti biometrici memorizzati informaticamente e direttamente confrontabile con altri *Template* Biometrici. Il *Template Biometrico* rappresenta la descrizione informatica sintetica della caratteristica biometrica ottenuta estraendo dal campione biometrico soltanto gli elementi salienti predefiniti;
- m) **Confronto Biometrico:** confronto, usualmente basato su metodi statistici e metriche tipiche del contesto tecnologico e del sistema biometrico prescelto, fra Dati Biometrici con l'obiettivo di stabilirne il grado di somiglianza o di dissomiglianza;
- n) **Corrispondenza:** la coincidenza, risultante da un confronto automatizzato, tra il *Template Biometrico* acquisito dai dispositivi dei sistemi di *Face Recognition* e i *Template* Biometrici derivanti dalle immagini dei candidati prenotati alle sessioni di esame previste nella giornata contenuti nel *Repository* immagini.

Art. 3

(Oggetto)



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

1. Il presente Decreto disciplina il Trattamento di Dati Personali riguardante l'utilizzo endoprocedimentale dei sistemi di *Face Recognition* ai fini dell'identificazione dei candidati che svolgono gli esami di teoria per conseguire le patenti di guida di cui all'articolo 116 commi 3, 4 e 11 del D.Lgs. 30 aprile 1992, n. 285;
2. Con riferimento ai profili tecnici, gli stessi sono contenuti nell'ambito dell'Allegato tecnico «*Principali garanzie e misure di sicurezza*».

Art. 4

(Finalità del presente Decreto)

1. La finalità del presente Decreto è quello di introdurre un nuovo sistema endoprocedimentale di riconoscimento dell'identità, già verificata *de visu* in occasione della visita medica preliminare alla presentazione della domanda d'esame, dei candidati prenotati per sostenere l'esame di teoria della patente di guida, per le categorie di cui all'art. 116 commi 3, 4 e della carta di qualificazione del conducente di cui all'art. 116 comma 11, basato sull'uso di dispositivi di acquisizione biometrica dotati di un *software* di riconoscimento facciale.

Art. 5

(Dati Personali acquisiti dai Sistemi di Face Recognition)

1. Per le finalità di cui al presente Decreto, i dispositivi utilizzati nell'ambito di entrambi i Sistemi di *Face Recognition* acquisiscono esclusivamente le immagini del volto dei candidati, le quali vengono immediatamente convertite in *Template* Biometrici non più riconducibili alla persona fisica, e cancellate in maniera irreversibile immediatamente dopo la creazione del *Template*.

Art. 6

(Modalità di funzionamento del Sistema Varco)

- 1) Il Sistema Varco consente il riconoscimento facciale dei candidati in sede di accesso ai locali preposti allo svolgimento dell'esame.
- 2) Il riconoscimento facciale avviene attraverso un confronto tra i Dati Biometrici del candidato, acquisiti dal dispositivo collocato in prossimità dei varchi di ingresso all'aula, e convertiti immediatamente in *Template* Biometrici, ed i *Template* Biometrici che il dispositivo ricava dalle immagini di tutti i candidati prenotati alle sessioni di esame previste nella giornata, contenute nel *Repository*.
- 3) Concluse le operazioni di accertamento dell'identità, in caso di esito positivo, il candidato potrà avere accesso all'aula d'esame. Qualora il Sistema Varco non dovesse, per qualsiasi ragione, riuscire ad effettuare il riconoscimento dell'interessato, l'esaminatore provvederà ad effettuare un riconoscimento a vista dello stesso.

Art. 7

(Modalità di funzionamento del Sistema Esame)

1. Il Sistema Esame consente il riconoscimento facciale dei candidati nella fase immediatamente antecedente l'avvio dell'esame e per tutta la durata dello stesso.
2. Le modalità di funzionamento del Sistema Esame si esplicano nelle seguenti fasi:
 - a) **Attivazione da parte del candidato del tasto "Procedi al riconoscimento"**: al fine dell'avvio della sessione d'esame, il candidato digita il pulsante "*Procedi al Riconoscimento*" sull'apposito dispositivo informatico presente nella postazione assegnatagli. Alla digitazione del comando, i *Template* Biometrici ricavati dalle immagini dei candidati prenotati alle sessioni di esame previste



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

nella giornata, contenute nel *Repository*, vengono acquisite dal dispositivo in quanto necessarie per il successivo Confronto Biometrico;

- b) **Acquisizione da parte del dispositivo dell'immagine del volto del candidato:** il dispositivo attiva la *Web-Cam* al fine dell'acquisizione dell'immagine del volto del candidato. L'immagine acquisita dalla telecamera viene conservata per gli istanti strettamente necessari alla sua codifica in *Template Biometrico*;
- c) **Verifica della corrispondenza prima dell'inizio dell'esame:** il *Template Biometrico* di cui alla precedente lettera b) viene utilizzato dal Sistema per effettuare la verifica dell'identità del candidato al fine di consentirgli di accedere all'esame, attraverso un confronto con tutti i *Template Biometrici* dei candidati, previamente acquisiti dal dispositivo nella fase di cui al punto a). Una volta verificata la corrispondenza, il Sistema cancella i *Template* non corrispondenti a quello del candidato e conserva esclusivamente quello corrispondente, utile per i successivi confronti;
- d) **Verifica della corrispondenza durante l'intera durata dell'esame:** il Sistema, attraverso il dispositivo, per tutta la durata dell'esame acquisisce, a intervalli regolari, le immagini del volto del candidato, che vengono codificate immediatamente in *Template Biometrici*. Tali *Template* vengono di volta in volta confrontati con il *Template Biometrico* derivante dal *Repository*, individuato e conservato nella fase di cui al punto c).

Art. 8

(*Tempi di conservazione dei dati*)

1. I dati oggetto di trattamento sono conservati per il periodo di tempo strettamente necessario a perseguire gli scopi per i quali sono stati raccolti e trattati. I tempi di conservazione dei dati nell'ambito di ciascun Sistema sono dettagliati nell'Allegato Tecnico.
2. I Campioni Biometrici impiegati per la realizzazione del *Template Biometrico* sono trattati solo durante le fasi di registrazione e di acquisizione necessarie al confronto biometrico e non sono memorizzati se non per il tempo strettamente necessario alla generazione del *Template*. I *Template Biometrici* verranno cancellati immediatamente in modo irreversibile secondo quanto previsto dall'Allegato Tecnico.
3. Nel caso in cui dovessero verificarsi episodi per i quali potrebbe rendersi necessario presentare una segnalazione alle competenti autorità giudiziarie, i dati potranno essere conservati su indicazione dell'esaminatore con modalità tecniche da individuare. Ai fini di tale conservazione saranno adottate apposite ed ulteriori garanzie per i diritti degli interessati.

Art. 9

(*Ruoli dei soggetti coinvolti nel Trattamento di Dati Personali*)

1. Il Ministero delle infrastrutture e della mobilità sostenibile è Titolare del Trattamento dei Dati Personali disciplinato dal presente Decreto.
2. Per la realizzazione e la gestione dei Sistemi, il Ministero può fare ricorso a soggetti terzi, previamente nominati Responsabili del trattamento, ai sensi dell'articolo 28 del GDPR.
3. Gli operatori incaricati di svolgere eventuali operazioni di manutenzione dei Sistemi di *Face Recognition* sono espressamente autorizzati, ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del D.Lgs. n. 196/2003.

Art. 10

(*Principali garanzie e misure di sicurezza del Trattamento*)

1. Il Trattamento dei Dati Personali posto in essere è conforme ai principi di liceità, necessità, finalità, proporzionalità di cui all'articolo 5 del GDPR.



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

2. Al fine di garantire i principi di cui sopra, il Ministero implementa le principali garanzie e misure di sicurezza, appropriate e specifiche, finalizzate a tutelare i diritti fondamentali e gli interessi delle persone fisiche i cui dati sono coinvolti nelle attività dei Sistemi previste nel presente Decreto, ai sensi di quanto prescritto dall'articolo 32 del GDPR e dal D.Lgs. n.196/2003 nonché dalle «*Linee guida in materia di riconoscimento biometrico e firma grafometrica*» che costituiscono l'Allegato A al Provvedimento n. 513 del 12 novembre 2014 del Garante per la Protezione dei Dati Personali. I requisiti di sicurezza adottati, così come precisati nell'Allegato tecnico al presente Decreto, garantiscono, in ogni caso:
 - a) l'integrità e la riservatezza dei dati;
 - b) la sicurezza dei Sistemi;
 - c) il tracciamento delle operazioni effettuate sui Sistemi.
3. Le misure tecniche e organizzative implementate tengono conto in special modo dei rischi presentati dal Trattamento, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.
4. Al fine di consentire il tempestivo adeguamento delle misure di sicurezza adottate ad eventuali aggiornamenti tecnico informatici o a nuove disposizioni di legge, nonché al fine di recepire eventuali indicazioni dell'Autorità Garante per la Protezione dei Dati Personali, le relative modifiche tecniche saranno adottate con apposito decreto di modifica da parte del Ministero.
5. I Dati Personali oggetto di Trattamento non saranno in alcun caso trasferiti in territori extra-UE.

Art. 11

(Informativa agli Interessati ed esercizio dei diritti connessi)

1. I candidati possono in qualsiasi momento esercitare i diritti loro riconosciuti dagli articoli 15 e seguenti del GDPR, così come specificati nell'ambito dell'informativa agli stessi fornita ai sensi degli articoli 13 e 14 del medesimo GDPR.
2. Nel caso in cui dovesse verificarsi, per qualsiasi ragione, il mancato riconoscimento del candidato mediante il Sistema biometrico in fase di avvio dell'esame, il candidato potrà comunque sostenere l'esame previo accertamento da parte dell'esaminatore del riconoscimento del candidato seduto alla postazione di esame.

Art. 12

(Disposizioni finali)

1. L'introduzione dei nuovi Sistemi di cui agli articoli che precedono, avverrà con un programma di rilascio progressivo su tutti gli uffici di Motorizzazione del territorio a decorrere dal 25 ottobre 2022 fino al 31 gennaio 2023.
2. Il presente Decreto trova applicazione a decorrere dal giorno della relativa pubblicazione nella sezione "Amministrazione Trasparente" del sito *web* del Ministero delle infrastrutture e della mobilità sostenibile.

(Ing. Pasquale D'Anzi)



Ministero delle infrastrutture e della mobilità sostenibili

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

Allegato tecnico

«Principali garanzie e misure di sicurezza»

1. Introduzione

Il presente Allegato descrive le principali garanzie e misure di sicurezza dei Sistemi di *Face Recognition*, utilizzati dal Ministero delle infrastrutture e della mobilità sostenibili nell'ambito delle procedure di riconoscimento facciale necessarie a identificare i candidati che devono sostenere gli esami di teoria per le patenti di guida di cui all'articolo 116 comma 3, lett. a) -g) del D.Lgs. 30 aprile 1992, n. 285, recante «*Nuovo codice della strada*», in conformità alla normativa in materia di protezione dei dati personali e, in particolare, al Regolamento (UE) 2016/679 e al D.Lgs. 196/2003; nonché alle «*Linee Guida in materia di riconoscimento biometrico e firma grafometrica*» che costituiscono l'Allegato A al Provvedimento n. 513 del 12 novembre 2014 e al provvedimento «*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*», pubblicato nella G.U. n. 300 del 24 dicembre 2008 e successivamente modificato in base al Provvedimento del 25 giugno 2009, adottati dal Garante per la Protezione dei Dati Personali.

2. I Sistemi di *Face Recognition*

I Sistemi di *Face Recognition* vengono utilizzati al fine di garantire l'accesso alle aule di esame, e lo svolgimento dell'esame di teoria, ai soli candidati prenotati alle sessioni di esame previste nella giornata, che siano stati previamente identificati mediante riconoscimento facciale.

I Sistemi si distinguono in:

- a) Sistema Varco, volto a garantire l'accesso del candidato all'aula;
- b) Sistema Esame, volto a garantire l'accesso del candidato all'esame e il continuo riconoscimento del candidato medesimo per tutta la durata di svolgimento dell'esame.

In particolare:

- a) il Sistema Varco è caratterizzato da un dispositivo (a seguire, anche «*Tablet*») dotato di una *Web-Cam* incorporata che, posto in prossimità dei varchi di ingresso alle aule, effettua il riconoscimento facciale e consente l'accesso agli ambienti soltanto a chi deve sostenere l'esame in quella determinata data. A tal fine, la telecamera del *Tablet* acquisisce le immagini dei volti per gli istanti strettamente necessari («*near real time*») alla loro codifica in *Template Biometrico* (a seguire, anche «**Codice Numerico Cifrato**» o «**Codice**»), il quale non sarebbe più riconducibile a Dati Personali del candidato. Il *Template Biometrico*, generato dall'acquisizione dell'immagine del volto del singolo candidato, viene confrontato con i *Template Biometrici* ricavati dalle immagini di tutti i candidati prenotati alle sessioni di esame previste in quella giornata, contenute nel *Repository* immagini, acquisiti dal *Tablet* con processo di *batch* notturno e cancellati al termine di tutte le sessioni di esame previste nella giornata.
- b) Il Sistema Esame è caratterizzato da un dispositivo (di seguito, anche «*Thin-Client*») presente nella postazione di esame, dotato di una *Web-Cam* che acquisisce le immagini del volto del candidato e le codifica in *Template Biometrici* al fine di effettuare il Confronto Biometrico.

Il Confronto Biometrico avviene prima dell'inizio dell'esame e durante tutta la durata dello stesso. Nello specifico:



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

- prima dell'inizio di ciascuna sessione di esame, alla digitazione, da parte del candidato, del tasto "Procedi al riconoscimento", il *Thin-Client* acquisisce i *Template* Biometrici ricavati dalle immagini di tutti i candidati prenotati alle sessioni di esame previste nella giornata, contenute nel *Repository* immagini;
- sempre in ragione della digitazione del tasto "Procedi al riconoscimento" il dispositivo attiva la *Web-Cam* ai fini dell'acquisizione dell'immagine del volto del candidato, che viene immediatamente convertita in *Template Biometrico*;
- a questo punto, all'interno del dispositivo, avviene il confronto tra il *Template Biometrico* acquisito dalla *Web-Cam* e tutti i *Template* Biometrici dei candidati prenotati alle sessioni d'esame di quel giorno, che il *Thin-Client* ha acquisito in precedenza (v. punto precedente);
- una volta individuato il *Template Biometrico* corrispondente a quello del candidato seduto nella postazione, il Sistema provvede a cancellare i *Template* non corrispondenti, conservando esclusivamente quello utile ad effettuare i successivi confronti per l'intera durata dell'esame;
- durante lo svolgimento dell'esame, la *Web-Cam* acquisisce, a intervalli regolari, l'immagine del volto del candidato, trasformandola in *Template Biometrico*, e confronta quest'ultimo con il *Template Biometrico* rimasto conservato nel *Thin-Client* all'esito del primo confronto.
- finito l'esame, vengono cancellati dal dispositivo tutti i *Template* Biometrici utilizzati.

3. Funzionalità dei Sistemi di *Face Recognition*

Si riporta a seguire la specificazione delle principali caratteristiche di entrambi i Sistemi, con particolare riferimento alle modalità di acquisizione, utilizzo e archiviazione dei Dati Biometrici e alla durata della loro eventuale conservazione:

- a) la fase di acquisizione e di memorizzazione del Dato Biometrico (c.d. *enrollment*) prevederà:
 - l'utilizzo di tecnologie idonee a garantire la correttezza dell'accreditamento nei Sistemi biometrici, il legame con il soggetto che si sottopone all'*enrollment* e la qualità del campione biometrico risultante;
 - l'immediata conversione dell'immagine acquisita in un *Template Biometrico* consistente in un Codice, attraverso un "procedimento di criptazione unidirezionale", e dunque senza la memorizzazione dell'immagine del volto. Tale processo non sarà reversibile e non sarà possibile in alcun modo ottenere l'immagine del volto a partire dal Codice;
 - la cifratura del Dato Biometrico al momento della sua acquisizione dal sensore, al fine di ridurre il rischio di acquisizione fraudolenta mediante attacchi informatici sul sensore o sui suoi canali di comunicazione con il Sistema biometrico;
 - la cancellazione dei Dati Biometrici grezzi, generati nel corso del procedimento di acquisizione biometrica, dalle aree di memoria temporanea, centrale e secondaria e dal *filesystem* del Sistema utilizzato per l'acquisizione, immediatamente dopo la generazione del *Template Biometrico*;
 - la memorizzazione e la conservazione dei *Template* Biometrici saranno effettuate dal Titolare, rispettivamente:
 - nell'ambito del Sistema Varco:
 - i *Template* Biometrici derivanti dalle immagini del volto acquisite dal *Tablet* vengono memorizzati per un tempo sufficiente al Confronto Biometrico (meno di 2 secondi), essendo gli stessi cancellati immediatamente dopo il confronto, a prescindere dal risultato dello stesso;



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

- i *Template* Biometrici di tutti i candidati prenotati alle sessioni di esame previste in quella giornata, ricavati dalle immagini contenute nel *Repository*, vengono cancellati al termine di tutte le sessioni d'esame previste nella giornata.
 - o nell'ambito del Sistema Esame:
 - i *Template* Biometrici del candidato, acquisiti dalla *Web-Cam* prima e durante lo svolgimento dell'esame, vengono conservati presso la postazione del candidato per un tempo corrispondente all'esecuzione dell'esame (30 minuti);
 - il *Template* Biometrico del candidato, ricavato dall'immagine contenuta nel *Repository*, che risulta corrispondente all'esito del primo Confronto Biometrico necessario ai fini dell'accesso del candidato all'esame, viene conservato presso la postazione del candidato per un tempo corrispondente all'esecuzione dell'esame (30 minuti), al fine di consentire i successivi confronti;
 - i *Template* Biometrici di tutti gli altri candidati prenotati alle sessioni di esame previste nella giornata, ricavati dalle immagini contenute nel *Repository*, vengono cancellati dal dispositivo al termine del primo Confronto Biometrico.
 - la trasmissione dei dati, sia in fase di *enrollment* sia in fase di riconoscimento, su canali di comunicazione cifrati tra il dispositivo di acquisizione e il Sistema su cui sono effettuati i Confronti Biometrici, nonché tra il *Repository* e il Sistema.
- b) ai fini della gestione e dell'utilizzo dei Sistemi, è previsto che:
- la rilevazione biometrica, finalizzata a garantire l'accesso all'esame da parte dei candidati, sia effettuata, nell'ambito di entrambi i Sistemi, mediante una modalità di riconoscimento con "confronto uno a molti", ossia basata sulla identificazione biometrica (processo in cui il soggetto dichiara la sua identità e il Sistema effettua un confronto fra il *Template* Biometrico estratto e quelli memorizzati nel *Repository*);
 - i dati relativi al numero di accessi ai Sistemi saranno conservati per il periodo di tempo strettamente necessario al perseguimento degli scopi per i quali i dati stessi sono raccolti e successivamente trattati;
 - i dati oggetto di trattamento per mezzo dei Sistemi saranno trattati per le sole finalità che il Ministero intende legittimamente perseguire, previamente indicate nell'informativa che verrà tempestivamente resa agli interessati, e non saranno utilizzati in altre operazioni di trattamento che siano con queste incompatibili;
 - saranno adottate misure volte a garantire ai candidati l'esercizio dei diritti previsti dagli articoli 15 e seguenti del Regolamento (UE) 2016/679.

4. Analisi dei rischi

Si è proceduto alla previa **analisi dei rischi** connessi all'utilizzo del Sistema, i cui esiti si riportano in sintesi nella tabella che segue, contenente la descrizione dei rischi potenziali e l'individuazione del livello di rischio, calcolato sulla base della gravità e della probabilità che i rischi si verifichino:

| TIPOLOGIA DI RISCHIO | DESCRIZIONE | LIVELLO DI RISCHIO | MISURE PREVENTIVE |
|--|---|--------------------|--|
| Rischio di non accuratezza del riconoscimento biometrico | È il rischio che, in fase di identificazione dell'Interessato, si verifichino falsi rigetti (o "falsi | BASSO | Misure di cui ai punti (i) e (ii) della sezione 5) |



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

| | | | |
|---|--|-------|--|
| | negativi”) o false accettazioni (o “falsi positivi”). | | |
| Rischio di falsificazione biometrica | È il rischio connesso alla creazione di un campione biometrico che, sottoposto allo stesso processo di estrazione delle minuzie, produca un <i>Template Biometrico</i> molto simile a quello iniziale. | BASSO | Misura di cui al punto (ii) della sezione 5) |
| Rischio di perdita accidentale di dati | Tale rischio è riconducibile a problemi di funzionamento dei sistemi informatici o a condotte umane non corrette, che possono comportare la perdita o la distruzione accidentale di dati. | BASSO | Misura di cui al punto (i) della sezione 5) |
| Rischio di furto o scambio di identità biometrica | È il rischio che ad un soggetto siano associati Dati Biometrici appartenenti ad altro soggetto. | BASSO | Misure di cui ai punti (i) e (iii) della sezione 5) |
| Rischio di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta | Tali rischi, che possono verificarsi a seguito di accessi non autorizzati al Sistema o per via di condotte scorrette (dolose o colpose) dei responsabili/incaricati, costituiscono profili da presidiare con estrema attenzione, anche in considerazione dei continui progressi dell’informatica e, conseguentemente, dei correlati rischi di “attacchi” da parte di soggetti non autorizzati, finalizzati al furto, alla sostituzione o alla distruzione di dati. | MEDIO | Misure di cui ai punti (i), (ii) (iii), (iv), (v) della sezione 5) |

5. Misure di sicurezza adottate ai fini del

Si riportano a seguire le principali **misure preventive** che saranno adottate al fine di presidiare i rischi sopra individuati:

- (i) **Misure di sicurezza relative al Trattamento Biometrico (par. 8.1 delle Linee Guida):** i dati oggetto di trattamento saranno custoditi e controllati utilizzando i mezzi tecnici attualmente a disposizione nel settore informatico, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di furto, sostituzione, distruzione o perdita, anche accidentale, dei dati stessi, nonché



Ministero delle infrastrutture e della mobilità sostenibili

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, ai sensi di quanto prescritto dall'art. 32 del Regolamento (UE) 2016/679.

In particolare, oltre alle **misure minime** di sicurezza previste in caso di trattamenti con strumenti elettronici, saranno adottate anche **misure ulteriori**, volte a prevenire i potenziali rischi specifici relativi al trattamento dei dati, anche alla luce di quanto prescritto nel paragrafo 8 delle Linee Guida del Garante.

Per ciò che concerne le **misure minime**, occorre distinguere:

▪ **con riferimento al Sistema Varco:**

- sono adottate procedure di autenticazione informatica idonee a prevenire il rischio di accessi al Sistema da parte di soggetti non autorizzati, e nello specifico:
 - un sistema di *Identity & Access Management* per l'identificazione dell'utente e della postazione, la gestione dei profili autorizzativi, la verifica dei diritti di accesso, il tracciamento delle operazioni attraverso un controllo accessi al *Repository* delle immagini eseguito a livello di *Active Directory*;
 - utenze *Windows* personali, definite con opportuno profilo autorizzativo e soggette ad un processo di approvazione da parte della sicurezza;
 - abilitazione *log auditing* su *host Windows* e invio Log a Connettore "*ArcSight*" dedicato all'applicazione *Driving Exams*.
- viene verificata con cadenza almeno annuale la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
- sono adottate ulteriori misure di sicurezza quali:
 - sistemi di sicurezza per la protezione delle informazioni;
 - la funzione "*Analisi delle Anomalie Applicative*" su *Driving Exams*, al fine di individuare usi anomali dell'applicazione implementata, in base a delle regole di correlazioni concordate;
 - sulla postazione dell'esaminatore e sul *Repository* delle immagini è installato un *software* antivirus che aggiorna in *real time* il *pattern* di possibili infezioni;
 - è effettuato l'aggiornamento dei programmi volti a prevenire la vulnerabilità attraverso *patching* semestrale.

▪ **con riferimento al Sistema di Accesso e Riconoscimento all'Esame:**

- sono adottate procedure di autenticazione informatica idonee a prevenire il rischio di accessi al Sistema da parte di soggetti non autorizzati, e nello specifico:
 - utenze amministrative personali sulla postazione "*Ubuntu*" su cui gira l'applicazione candidato, definite con opportuno profilo autorizzativo e soggette ad un processo di approvazione da parte della sicurezza;
 - un sistema di tracciamento e di conservazione dei dati di accesso alle componenti "Esaminatore" e "Candidato", implementato per l'applicazione *Driving Exams*.
- le postazioni esame sono configurate in modalità "*Kiosk*". La modalità *Kiosk* consente di bloccare le principali funzioni del dispositivo per proteggerlo dalle azioni degli utenti. Non sono presenti sistemi di I/O come tastiera e *mouse* e le porte *USB* sono disabitate durante il corso dell'esame;



Ministero delle infrastrutture e della mobilità sostenibile

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

- sono effettuate, con cadenza almeno semestrale, aggiornamenti dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Con riferimento alle **misure ulteriori**, saranno previste a titolo esemplificativo le seguenti misure:

- la lista dei soggetti autorizzati che potranno accedere ai dati sarà semestralmente rivista in base alle effettive esigenze lavorative;
- mensilmente verrà effettuato un controllo al fine di verificare che le utenze siano effettivamente solo quelle autorizzate nell'ambito del processo di nomina dei soggetti autorizzati;
- sui *database* che ospiteranno i dati sarà attivato l'*auditing* al fine di tracciare eventi di accesso, modifica e cancellazione dei dati, tali eventi saranno conservati sulla piattaforma di *Log Management* anche in conformità a quanto previsto dal Provvedimento del Garante sugli Amministratori di Sistema;
- saranno attivati degli allarmi sulla piattaforma di correlazione degli eventi al fine di intercettare accessi o operazioni non autorizzate sui Dati Biometrici effettuati con strumenti di amministrazione dei *database*;
- saranno effettuati *vulnerability assessment* sistemistici volti a verificare la corretta configurazione dei *database* che ospitano i Dati Biometrici;
- saranno effettuati *vulnerability assessment* applicativi volti a simulare tentativi di accesso e modifica dei Dati Biometrici e quindi a verificare la robustezza delle contromisure implementate per garantirne la loro riservatezza e integrità.

(ii) Misure di sicurezza relative ai Sistemi biometrici (par. 8.2 delle Linee Guida): saranno impiegate modalità tecniche per l'acquisizione dei Dati Biometrici che, come previsto dal paragrafo 8.2 delle Linee Guida:

- cancellino irreversibilmente i Dati Biometrici grezzi (le immagini del volto) e prevedano la trasmissione dei dati, sia in fase di *enrollment* che in fase di acquisizione dal *Repository*, solo su canali di comunicazione cifrati;
- acquisiscano il numero di informazioni strettamente necessario all'identificazione dell'Interessato, in modo da rendere impossibile la ricostruzione del Campione Biometrico originario;

(iii) Modalità di memorizzazione e gestione dei dati (par. 8.3 delle Linee Guida): relativamente a tale profilo, come previsto dal paragrafo 8.3 delle Linee Guida, i *Template* Biometrici, per il tempo della loro conservazione, saranno conservati in *database* che supportino la cifratura a livello di colonna e i dati identificativi degli utenti saranno conservati separatamente dai relativi Dati Biometrici.

La conservazione dei *Template* Biometrici sarà effettuata mediante l'adozione di misure tecniche, quali descritte nel presente paragrafo sub i), volte a prevenire i rischi di accesso non autorizzato, furto, sostituzione o compromissione dei Dati Biometrici.

(iv) Registrazione degli accessi ai Dati Biometrici (par. 8.4 delle Linee Guida): saranno adottati sistemi idonei alla registrazione degli accessi da parte dei soggetti specificatamente abilitati a svolgere mansioni tecniche connesse alla manutenzione e alla gestione dei Sistemi, che dovranno essere, a tal fine, appositamente autorizzati. Tali registrazioni comprenderanno i riferimenti temporali e avranno caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i *log* degli accessi di cui al provvedimento del Garante sugli amministratori di sistema;



Ministero delle infrastrutture e della mobilità sostenibili

DIPARTIMENTO PER LA MOBILITA' SOSTENIBILE

DIREZIONE GENERALE PER LA MOTORIZZAZIONE, PER I SERVIZI AI CITTADINI
E ALLE IMPRESE IN MATERIA DI TRASPORTI E NAVIGAZIONE

IL DIRETTORE GENERALE

(v) **Tempi di conservazione dei Dati Biometrici (par. 8.5 delle Linee Guida):** i Dati Biometrici rilevati saranno oggetto di trattamento per il periodo di tempo strettamente necessario a perseguire gli scopi per i quali sono stati raccolti e trattati. In particolare:

▪ **nell'ambito del Sistema Varco:**

- i dati grezzi impiegati per la realizzazione, tramite la *Web-Cam* del *Tablet* di accesso, del *Template* Biometrico non saranno memorizzati se non per il tempo strettamente necessario alla generazione del *Template* Biometrico;
- i *Template* Biometrici realizzati tramite la *Web-Cam* del *Tablet* di accesso sono conservati per un tempo sufficiente al confronto (meno di due secondi) e vengono cancellati immediatamente dopo;
- i *Template* Biometrici provenienti dal *Repository* sono conservati per la giornata di esami.

▪ **nell'ambito del Sistema Esame:**

- i dati grezzi impiegati nella realizzazione, tramite la *Web-Cam* del *Thin-Client*, del *Template* Biometrico non saranno memorizzati se non per il tempo strettamente necessario alla generazione del *Template*;
- nel *Thin-Client*, a cui accede il candidato:
 - i *Template* Biometrici acquisiti tramite la *Web-Cam* del *Thin-Client* durante l'esame sono conservati per tutta la durata dell'esame;
 - i *Template* Biometrici, acquisiti dal *Repository*, di tutti i candidati che, all'esito del confronto, non corrispondono al *Template* Biometrico del candidato che deve sostenere l'esame, vengono cancellati immediatamente dopo il confronto;
 - il *Template* Biometrico, acquisito dal *Repository*, che all'esito del confronto corrisponde al *Template* Biometrico del candidato che deve sostenere l'esame, viene conservato per la durata dell'esame (trenta minuti).

Una volta venuta meno la necessità di trattamento, tutti i dati sono cancellati in modo sicuro e irreversibile.