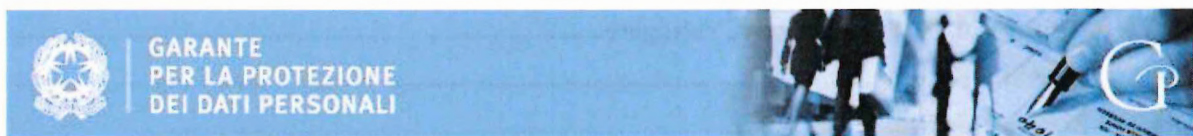


ISFORT S.P.A.
Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA



**Documento di valutazione
d'impatto sulla protezione dei dati**

(Data Protection Impact Assessment – DPIA)

e Registro dei Trattamenti

(in ottemperanza al REGOLAMENTO UE 2016/679)

Istituto Superiore di Formazione e Ricerca per i Trasporti

ISFORT S.p.A.

Data ultima revisione

documento: 15/10/2021

Il titolare del trattamento

Dr. Marco Romani

ISF	Dr. Marco Romani Titolare del Trattamento	Data:	15/10/2021	File:	D P I A 2020.doc
------------	---	--------------	-------------------	--------------	------------------

Sommario

1. Premessa	3
2. Principali Riferimenti Legislativi.....	10
3. Composizione del documento	11
4. Identificazione delle Risorse da Proteggere.....	17
4.1 Luoghi Fisici.	18
4.2 Risorse Hardware.	23
4.3 Risorse dati.	42
4.4 Risorse software	48
5. Analisi dei Rischi	56
5.1 ANALISI DEI RISCHI SUI LUOGHI FISICI	56
5.2 ANALISI DEI RISCHI SULLE RISORSE HARDWARE.....	57
5.3 ANALISI DEI RISCHI SULLE RISORSE DATI	58
5.4 ANALISI DEI RISCHI SULLE RISORSE SOFTWARE	60
6. Definizione ed attuazione della Politica di Sicurezza	61
6.1 MISURE DI SICUREZZA ADOTTATE DI TIPO FISICO.....	62
6.2 MISURE DI SICUREZZA ADOTTATE DI TIPO LOGICO	64
6.3 MISURE DI SICUREZZA ADOTTATE DI TIPO ORGANIZZATIVO.....	66
7. Piano di verifica delle Misure Adottate e Registro dei trattamenti.....	69
9. Appendice: Soglie di Rischio.....	74
ALLEGATI	75

1. Premessa

Istituto Superiore di Formazione e Ricerca per i Trasporti ed in breve Isfort S.p.A (in seguito Istituto) è stato costituito nel 1994, per iniziativa dell'Ente Banca Nazionale delle Comunicazioni e delle Ferrovie dello Stato Italiane, che insieme ne rappresentano la compagine societaria, con la finalità di contribuire al processo di rinnovamento del settore della mobilità di persone, merci e informazioni.

In coerenza con la propria missione statutaria l'Istituto si propone di supportare lo sviluppo del know-how socio-economico e gestionale del settore, attraverso attività sistematiche e mirate di ricerca e formazione.

Tre impostazioni di fondo caratterizzano le attività di :

- la focalizzazione tematica sull'ascolto, la lettura, l'interpretazione della domanda di mobilità, degli individui e delle imprese, attraverso l'esplicitazione di bisogni ed esigenze, la ricostruzione di stili e comportamenti, il monitoraggio strutturale e congiunturale, la definizione di policy appropriate, aderenti al "punto di vista" dei consumatori di mobilità;
- la costante tensione esplorativa verso i fatti innovativi e le emergenti fenomenologie economiche e sociali che interessano i sistemi di mobilità di persone e merci, nonché le reti e il territorio;
- lo sviluppo di strumenti per la pianificazione dei trasporti, sia nei diversi livelli territoriali che modali (dai Piani Urbani della Mobilità Sostenibile ai piani di settore), con particolare riferimento alla pianificazione e alla programmazione dei servizi di Trasporto Pubblico Locale.

L'approccio di Isfort è caratterizzato, dunque,

- dalla valorizzazione degli strumenti di indagine di campo, per il focus sulla comprensione in profondità dei processi reali, per l'individuazione di un corretto equilibrio tra aspetti quantitativi e sviluppo delle dimensioni più qualitative dell'analisi;
- dalla utilizzazione di rigorosi strumenti matematici finalizzati alla modellizzazione dei fenomeni, alla formulazione di scenari previsionali, alla valutazione dell'impatto sui sistemi di trasporto e sull'ambiente di nuove infrastrutture e di nuovi servizi di mobilità.

Nell'ambito dell'**area ricerca** Isfort produce conoscenze scientifiche nel settore dei trasporti, con la finalità di promuovere una più moderna e diffusa cultura della mobilità, con l'obiettivo di leggere e interpretare i fenomeni e le tendenze più rilevanti del settore, identificare i problemi critici e progettare strumenti operativi e modelli di comportamento appropriati per affrontarli.

Nello specifico nelle attività istituzionali di ricerca rientrano i programmi che, finanziati dalla Fondazione NC, azionista di controllo, e/o da altre parti interessate, rispondono alla esigenza della Fondazione stessa di perseguire gli obiettivi previsti dalla propria mission. Tali attività sono riconducibili

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

ai tre **Osservatori sulla Mobilità** e ai progetti specifici richiesti di anno in anno. L'elaborazione dei dati dell'**Osservatorio "Audimob"**, giunto alla 20a edizione, con gli aggiornamenti delle rilevazioni 2018 e del primo semestre 2019, permette di leggere in profondità le caratteristiche e le dinamiche degli stili e dei comportamenti di mobilità degli italiani.

Da tempo, peraltro, le risultanze delle rilevazioni di Isfort su questo tema sono entrate a far parte del Conto Nazionale dei Trasporti e delle previsioni del **Programma Statistico Nazionale** cui l'Istituto invia gli aggiornamenti annuali dell'Osservatorio Audimob, in quanto inserito nel Sistema Statistico Nazionale - SISTAN – dell'Istat con provvedimento della Presidenza del Consiglio dei Ministri del 14 marzo 2012. L'Osservatorio Audimob è inserito anche nel **Programma Statistico Nazionale 2020 – 2022**.

Nell'ambito dell'**area formazione** l'Istituto progetta e realizza interventi finalizzati allo sviluppo della cultura e delle competenze gestionali in imprese e istituzioni operanti principalmente nel settore della mobilità.

Tra le priorità di questi interventi si colloca lo sviluppo tecnico-gestionale del settore anche attraverso la produzione di servizi di formazione e qualificazione tecnico-professionale che la Società – ai sensi del proprio statuto - programma, organizza e realizza in proprio e avvalendosi di terzi.

In linea di principio le iniziative di formazione, pertinenti gli ambiti di attività istituzionale di Isfort, rientrano nelle competenze e responsabilità della Direzione Ricerca di ISFORT mentre i **corsi, a livello nazionale riservati agli Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario** sono competenza della specifica struttura dell'Istituto, di seguito denominata **Direzione Formazione Attività Sicurezza Ferroviaria** (in breve **CdF**) con i ruoli e le responsabilità previsti secondo le Linee Guida **dell'Agenzia Nazionale per la Sicurezza delle Ferrovie**, ANSF, ente pubblico sottoposto ai poteri di indirizzo e vigilanza del Ministro delle infrastrutture e dei trasporti e al controllo della Corte dei Conti. Dette Linee Guida sono esplicitate nel documento dell'ANSF del 27 ottobre 2010 a cui Isfort deve conformarsi per mantenere il riconoscimento nel Pubblico Registro dei Centri di Formazione.

Si annota, altresì, che, con il fine di dare all'Istituto un quadro di *governance* societaria efficace, soprattutto in termini di vigilanza sull'applicazione dei principi di buona gestione aziendale sia nei riguardi degli utenti e committenti dei servizi sia degli stakeholders la Società si è dotata di un **Sistema di Gestione per la Qualità (SGQ)** sottoponendo a certificazione tutti i processi di gestione del prodotto della ricerca e dei servizi ai clienti col fine di migliorarne continuamente la qualità.

Al termine del processo di certificazione è stato redatto il **Manuale della Qualità (MQ)** con lo scopo di descrivere l'organizzazione e le attività operative per realizzare la Qualità secondo i punti della **normativa UNI EN ISO 9001:2015** e le proprie modalità gestionali, finalizzato a garantire idonei livelli tecnico qualitativi per la soddisfazione dei committenti pubblici e privati e degli stakeholders.

L'applicazione del SGQ è un impegno pienamente condiviso ed approvato dalla direzione aziendale.

Un SGQ applicato nell'espletazione delle proprie peculiari attività consente alla Società di mantenere elevati e controllati gli standard.

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

Strettamente connessa con il citato impegno di corretta applicazione delle buone pratiche di *governance* aziendale, in applicazione del principio di *accountability*, richiesta dal dettato comunitario, Isfort non poteva esimersi da una attenta revisione delle **procedure di tutela del dato personale** a seguito dell'entrata in vigore, il 25 maggio 2018, del **Regolamento UE 2016/679 – GDPR**.

Riguardo alle norme relative al trattamento dei dati personali, l'Istituto aveva ottemperato al dettato del previgente D.Lgs. 196/2003, adottando il DPSS – Documento programmatico sulla Sicurezza, nominando il Responsabile del Trattamento, l'Amministratore di Sistema e i delegati al trattamento.

In ragione di quanto sopra gli uffici dell'Istituto erano stati dotati di accessi, armadi, cassettiere con serramenti protetti, specifiche procedure organizzative e di una rete informatica LAN, finalizzata ad autorizzare l'accesso a specifiche banche dati elettroniche ai soli incaricati a quel specifico trattamento, tramite apposite credenziali di accesso e opportune procedure di sicurezza poste in essere anche in relazione agli aspetti riguardanti il *backup* e il *disaster recovery*.

Successivamente, con il venire meno degli obblighi relativi alla predisposizione del DPSS, previsto dall'art. 34 del D.Lgs 196/2003, abrogato con il D.L. 5/2012, convertito nella legge 35 del 4 aprile 2012, l'Istituto ha ritenuto di continuare ad aggiornare gli ambiti dei trattamenti (cartacei ed elettronici) dei dati personali, mantenendo le figure responsabili precedentemente nominate, gli incaricati e l'Amministratore del sistema informatico, che esegue le attività di controllo circa l'uso degli strumenti elettronici interni e delinea le *policies* della sicurezza informatica.

Con l'entrata in vigore, il 25 maggio 2018, del **Regolamento UE 2016/679 – GDPR**, ha verificato la propria posizione in relazione agli adempimenti previsti, giungendo a valutare in misura diversa le proprie attività istituzionali ai fini del trattamento dei dati personali svolto presso i propri uffici, sia per categorie di interessati, sia per tipologia e dimensione dei dati raccolti sia per diffusione territoriale.

Al completamento di questa attività di monitoraggio si è giunti a determinare che sia per le attività istituzionali in genere che per le attività nell'area ricerca l'Istituto non raccoglie dati sensibili ma esclusivamente dati personali non sensibili, quali dati anagrafici, dati amministrativi, dati contrattuali, con la sola eccezione dei dati sensibili di natura medica, raccolti e gestiti ai fini della gestione del personale, che sono trattati e conservati presso il medico incaricato.

La sola eccezione è relativa ai dati raccolti per le attività di formazione regolata in ambito ANSF, svolte dalla Direzione Formazione Attività Sicurezza Ferroviaria (in breve CdF), di cui si dirà più avanti, relativamente ai corsi per **Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario, in conformità alle Linee Guida ANSF e alla Convenzione con Trenitalia S.p.A. del 19 ottobre 2017.**

Relativamente ai dati raccolti nell'area ricerca trattasi esclusivamente di dati non sensibili nell'ambito delle attività prevalenti dell'Istituto e la raccolta e il trattamento avviene, in ogni caso, a mezzo di una procedura informatizzata, soggetta a controllo. La predetta procedura prevede la dichiarazione che i dati sono raccolti e trattati al solo fine di gestione della operatività aziendale, con contestuale rilascio, direttamente o anche attraverso il sito Internet, di idonea informativa di legge sul trattamento dei dati effettuato e conseguente raccolta del consenso degli stessi interessati.

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

L'Istituto, inoltre, in ogni caso precisa che il trattamento dei predetti dati personali connessi agli adempimenti contabili e amministrativi, avviene su proprio server e tutte le attività informatiche collegate avvengono al proprio interno, con conseguente nomina del responsabile del trattamento di dati personali, per la parte di propria competenza.

Merita, in ogni caso, una specifica puntualizzazione relativamente alla raccolta dati, attraverso soggetti specializzati in indagini e ricerche di mercato, **finalizzati alla stesura dei rapporti annuali Audimob e altre ricerche istituzionali.**

La verifica delle modalità di raccolta e trattamento dati nell'ambito delle predette indagini statistiche ha consentito di escludere che in tali attività istituzionali si svolgano trattamenti di dati personali e, a maggior ragione, di categorie particolari di dati come specificato dal **Regolamento UE 2016/679 – GDPR.**

L'Isfort, infatti, affida la raccolta dei dati utili alle proprie indagini statistiche a soggetti terzi, con specifici incarichi, che tra le clausole espresse prevedono **l'impegno a fornire all'Istituto i risultati di ciascuna indagine in forma di microdati o aggregazioni di dati, in ogni caso esclusivamente anonimi e non riconducibili in alcun modo a persone fisiche.** I predetti incarichi prevedono, altresì, che a tale riguardo le agenzie incaricate si siano conformate alle previsioni del **Regolamento UE 2016/679 – GDPR e che di ciò diano atto nell'accettazione degli incarichi.**

Diverso è il risultato del monitoraggio per le attività di **formazione regolata**, erogate da Isfort per il tramite del proprio CdF, come Centro di formazione riconosciuto da ANSF, Agenzia Nazionale per la Sicurezza delle Ferrovie, che consentono di organizzare corsi per il rilascio della **Licenza europea per la condotta dei treni.**

Oltre alla Licenza, in particolare detti corsi sono finalizzati al :

- conseguimento del **Certificato complementare tipo A4+B1** (condotta di treni viaggiatori di lunga percorrenza, di trasporto locale, ecc.)
- conseguimento del **Certificato complementare tipo A4+B** (condotta di treni per trasporto viaggiatori e merci)
- mantenimento e recupero delle competenze

In ragione della verifica effettuata, **Isfort ha ritenuto di effettuare la valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA)** in applicazione del disposto della sezione 3 e degli artt. 27 e 35 del Regolamento UE 2016/679 – GDPR, e con particolare riferimento all'art. 9, comma 2, lettera d, del citato Regolamento, **esclusivamente su detta area di formazione regolata in quanto solo in essa si effettuano trattamenti di categorie particolari di dati personali finalizzati dell'inserimento dei candidati nei corsi di cui in precedenza.**

Nell'ambito del predetto processo di valutazione si è effettuata:

- la contestuale mappatura dei trattamenti effettuati dal Titolare
- la valutazione del rischio privacy
- la conduzione della DPIA per i soli trattamenti individuati come potenzialmente rischiosi

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45

00198 ROMA

- la definizione dei trattamenti individuati da notificare al garante della Privacy
- la predisposizione del Registro dei rischi Privacy
- la conseguente nomina del Responsabile della Protezione dei Dati (RPD/DPO) nella persona del dr. Pier Luigi Aymerich il cui atto di nomina è allegato al DPIA, con collegata comunicazione di legge al Garante della Privacy.

1.1. Organi societari

Presidente della Società

Avv. Prof. Marco Milli

Consiglio di Amministrazione

- Marco Milli - Presidente

- Marco Romani - Consigliere e Amministratore Delegato

- Andrea Pelle - Consigliere

- Maria Teresa De Benedictis - Consigliere

- Mario Tartaglia - Consigliere

Collegio dei Sindaci

Enrico Verri - Presidente

Alfredo Maccallini – Sindaco effettivo

Francesco Paolo Bellaroto – Sindaco effettivo

Ennio Celio Luglio – Sindaco Supplente

Giombi Giambartolomei Stefano – Sindaco Supplente

I Membri degli Organi societari sono tenuti per obbligo di mandato al pieno rispetto delle previsioni del Regolamento UE 2016/679 – GDPR per quanto riguarda i trattamenti di categorie particolari di dati personali di cui verranno a conoscenza nell'espletamento delle attività di loro competenza.

Parimenti l'Istituto si obbliga al medesimo rispetto per quanto attiene a categorie particolari di dati personali dei predetti Membri, di cui potrebbe venire a conoscenza per soli fini amministrativi e di gestione operativa della Società.

1.2 Personale e collaboratori

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

L'Istituto ha n.7 dipendenti e numero variabile (da 4 a 9 a seconda delle attività) di collaboratori esterni. I dati relativi al personale sono trattati secondo le norme del Regolamento UE 2016/679 – GDPR come dati personali non sensibili, quali dati anagrafici con la sola eccezione dei dati sensibili di natura medica raccolti e gestiti ai fini della gestione del personale, che sono trattati e conservati presso il medico incaricato.

L'organigramma della società è descritto nell'allegato n. 1.

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

1.3 Nomine e competenze ai fini del Regolamento UE 2016/679 – GDPR

Rappresentanti Legali di Isfort sono il Presidente Avv. Prof. Marco Milli (presidente@isfort.it) e l'Amministratore Delegato, Dr. Marco Romani (mromani@isfort.it)

L'Istituto ha nominato:

Titolare del Trattamento dei dati personali (TdT) e Responsabile della gestione del trattamento dei dati personali dell'Istituto (RdT/IS) il Dr. Marco Romani

Responsabile della gestione del trattamento dei dati personali del Centro di Formazione (RdT/CdF) l'Ing. Cesare Borgia (formazione@isfort.it)

Responsabile della Protezione dei Dati Personali (RPD/DPO)

il Dr. Pier Luigi Aymerich (aymerich@pec-legal.it)

Il Responsabile della sicurezza dei sistemi informativi (RSI) il Dr. Massimo Procopio (mprocopio@isfort.it)

Addetti al trattamento dati personali:

Sig.ra Angela Cesaroni Addetto Trattamento dati Istituto (AdT/IS) e dati Centro di Formazione (AdT/CdF/NIPS)

Sig.ra Daniela Campora Addetto Trattamento dati Istituto (AdT/IS)

Addetto Verifica Green Pass (AdT/VGP)

Sig. Valerio Tiberi Istruttore /Esaminatore Addetto Trattamento dati Centro di Formazione (AdT/CdF/NIP)

Sig. Paolo Paccosi Addetto Trattamento dati Centro di Formazione (AdT/CdF/RQ)

Gli Atti di Nomina sono allegati al presente Documento di valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA).

2. Principali Riferimenti Legislativi

- Direttiva 95/46/CE del 24 ottobre 1995 “Regolamento Generale sulla Protezione dei Dati – RGPD”
- Legge 31 dicembre 1996, n. 675 “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali” e successive disposizione correttive e integrative.
- Legge n. 127 del 24 marzo 2001
- Decreto legislativo 30 giugno 2003, n. 196
- Legge 26 febbraio 2004, n. 45
- Legge 27 gennaio 2006, n. 21
- Decreto legislativo 30 maggio 2008, n. 109
- Legge 20 novembre 2009, n. 166
- Legge 4 novembre 2010, n. 183
- Regolamento UE 2016/679 del 27 aprile 2016
- Comitato Europeo per la Protezione dei Dati del 25 maggio 2018 “WP248, rev. 01”
- Delibera 11 ottobre 2018, n. 467 del Garante per la Protezione dei Dati, G.U. n. 269 del 19.11.2018
- Decreto del Presidente del Consiglio dei Ministri del 17 giugno 2021
- Legge 17 giugno 2021, n. 87, di conversione del D.L. 22 aprile 2021, n. 52
- Decreto legge 21 settembre 2021, n. 127

3. Composizione del documento

Il presente documento è stato compilato, limitatamente alla raccolta e trattamento dei dati personali **che interessano la raccolta e trattamento dei dati personali nell'ambito delle attività di formazione regolata, erogata da Isfort per il tramite del proprio CdF, come Centro di formazione riconosciuto da ANSF, Agenzia Nazionale per la Sicurezza delle Ferrovie, che consente di organizzare corsi per il rilascio della Licenza europea per la condotta dei treni.**

La compilazione del documento è in applicazione del Regolamento UE 2016/679 – GDPR del 27 aprile 2016, che ha modificato e integrato la Direttiva 95/46/CE del 24 ottobre 1995 “Regolamento Generale sulla Protezione dei Dati – RGPD”.

Nel nostro ordinamento il dettato europeo è stato recepito con la Legge 31 dicembre 1996, n. 675 “Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali” e successive modificazioni e integrazioni, raccolte successivamente nel Decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali.

Per la specificità dei dati raccolti nell'ambito delle predette **attività di formazione regolata**, l'Istituto, in applicazione del disposto della sezione 3 e degli artt. 27 e 35 del Regolamento UE 2016/679 – GDPR, ha ritenuto di effettuare la valutazione dell'impatto del trattamento previsti sulla protezione dei dati personali (DPIA), e contestualmente tutti gli adempimenti connessi, come meglio specificato nel dettaglio alla pagina 6 del presente documento.

L'articolo 35, comma 1, del GDPR prevede che il processo di DPIA sia obbligatorio quando un trattamento di dati personali "presenti un rischio elevato per i diritti e le libertà delle persone fisiche". Sul punto, al fine di assicurare un'interpretazione coerente delle circostanze in cui risulta obbligatorio lo svolgimento di un DPIA, il gruppo di lavoro ex articolo 29 (gruppo di lavoro a cui fanno parte tutte le Authority Privacy di ciascun Stato Membro dell'Unione Europea c.d. "WP-29") ha chiarito, con il Documento WP248, rev.01, del 25 maggio 2018, i nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un rischio elevato. Il riferimento di base resta il rispetto dei "diritti e libertà" degli interessati e riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione. Qualora vi siano incertezze sulla obbligatorietà di effettuare un DPIA la raccomandazione del WP-29 è quella di effettuarlo comunque, in quanto si tratterebbe di uno strumento comunque utile per i titolari del trattamento.

In ogni caso l'articolo 35, comma 3, del GDPR definisce alcuni esempi i casi nei quali un trattamento di dati personali "possa presentare rischi elevati": (a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; (b) il trattamento, su larga scala, di categorie particolari di dati personali (articolo 9 del GDPR) o di dati relativi a condanne penali e a reati (cfr. articolo 10 del GDPR); (c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Con propria Delibera dell'11 ottobre 2018, n. 467, pubblicata in G.U. n. 269 del 19.11.2018, il Garante per la Protezione dei Dati, ha individuato, nell'Allegato 1, l'elenco delle tipologie di trattamenti da

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

sottoporre a valutazione d'impatto, che specificano quanto determinato dal già menzionato Documento WP248, rev.01.

Al punto 10 di detto Allegato sono inseriti i "trattamenti di categorie particolari di dati" ai sensi dell'art. 9 del Regolamento GDPR, in precedenza richiamato.

Al fine della compilazione del presente documento l'Istituto ha ritenuto di utilizzare come riferimento, per quanto applicabili, le indicazioni del precedente D.lgs 196/2003, che all'art. 34 indicava le misure minime di sicurezza come segue:

"Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime:

- a) autenticazione informatica a mezzo password;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato Documento di Valutazione di Impatto sulla protezione dei dati - DPIA;
- h) adozione di tecniche di cifratura o di codici identificativi, se del caso, per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

L'Istituto considera l'approvazione del Regolamento UE 2016/679 – GDPR del 27 aprile 2016, un ulteriore passaggio della tutela e protezione dei diritti personali così come garantito dall'art.8 della Carta dei Diritti Fondamentali dell'Unione Europea, una conquista civile di grande importanza atta a garantire la tutela dei dati personali di ciascun individuo.

In proposito si rammenta che il Regolamento comunitario è un atto vincolante per tutti gli stati membri, alla stregua di legge, e si caratterizza per tre elementi fondamentali: ha portata generale, essendo indirizzato a tutti i soggetti giuridici comunitari (Stati membri e persone fisiche e giuridiche degli Stati stessi), è obbligatorio in tutti i suoi elementi ed è direttamente applicabile.

Al fine di recepire completamente lo spirito con cui è stato varato il nuovo Regolamento, l'Istituto ha elaborato il seguente Documento di valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA), che testimonia lo sforzo fatto dalla nostra realtà al fine di garantire la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Il documento procede innanzitutto dalla **Identificazione delle Risorse da proteggere**, risorse che in diverso modo operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati personali. A questo proposito, tramite **l'Analisi dei Rischi**, sono state analizzate le minacce e le

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

vulnerabilità a cui tali risorse sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Valutati i rischi, si è redatto un **Piano di Sicurezza**, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi i dati stessi.

Inoltre è stato definito un **Piano di Verifiche** delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari e un conseguente **Registro dei Trattamenti**, anch'esso soggetto a periodiche verifiche e aggiornamenti.

Parallelamente alla stesura del **Piano di Verifiche** è stato redatto un **Piano di Informazione e condivisione degli obiettivi** tramite il quale si renderanno edotti gli incaricati del trattamento dei rischi e dei modi per prevenire i danni.

Contestualmente la Società si è già conformata alle prescrizioni dell'articolo 13 del Regolamento UE in merito alle **"informazioni agli interessati"**, adottando due modalità di conferimento di dette informazioni. Relativamente agli obblighi riferiti al trattamento di dati non sensibili la Società comunica il conferimento delle succitate informazioni, integralmente, attraverso il proprio sito e, in forma sintetica, in calce alle email inviate. Relativamente agli obblighi riferiti al **trattamento di categorie particolari di dati personali**, finalizzati dell'inserimento dei candidati nei **corsi di formazione regolata** in ambito ANSF, per Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario, acquisiti dalla Società tramite iscrizione degli interessati, Isfort comunica il conferimento delle succitate informazioni attraverso **idonea informativa**. Detta informativa contiene tutti gli elementi richiesti dal citato art. 13 della norma europea e viene consegnata contestualmente alla domanda di iscrizione, e se ne richiede la sottoscrizione da parte degli interessati. Relativamente al conferimento delle informazioni ex articolo 14 del Regolamento (UE) n. 2016/679 Isfort rammenta che per quanto attiene alla attività nell'**ambito dell'area ricerca** l'Istituto non raccoglie categorie particolari di dati ma esclusivamente **dati personali non sensibili**. La raccolta e il trattamento dati di ricerca avviene esclusivamente attraverso soggetti specializzati in indagini e ricerche di mercato, finalizzati alla stesura dei rapporti annuali Audimob e altre ricerche istituzionali. Si ribadisce, peraltro, che la Società affidando la raccolta dei dati utili alle proprie indagini statistiche a soggetti terzi, con specifici incarichi, che tra le clausole espresse prevedono l'impegno a fornire all'Istituto i risultati di ciascuna indagine in forma di microdati o aggregazioni di dati, in ogni caso esclusivamente anonimi e non riconducibili in alcun modo a persone fisiche, non ha necessità di predisporre specifiche modalità di conferimento delle informazioni a norma del citato art. 14 **non avendo disponibile alcun dato personale dei soggetti interessati**. I predetti incarichi alle agenzie di ricerca prevedono, altresì, che dette agenzie incaricate si conformino alle previsioni del Regolamento UE 2016/679 – GDPR e che di ciò diano atto nell'accettazione degli incarichi, provvedendo in via autonoma all'informativa di legge ai soggetti interessati.

Gli obblighi ex artt. 13 e 14 del Regolamento Europeo ("informazioni agli interessati") saranno ampiamente condivisi con tutti gli incaricati, ai quali saranno fornite specifiche istruzioni in merito alla obbligatorietà di garantire l'esercizio dei diritti degli interessati.

Sempre in sede di monitoraggio delle attività dell'azienda, ai fini della redazione della DPIA, avuto riguardo dei trattamenti descritti in precedenza, si sono valutate non necessarie misure e tecniche di cifratura e pseudonimizzazione così come non essendo effettuate in azienda attività che coinvolgono categorie vulnerabili di interessati non è stata valutata come necessaria l'adozione di specifiche misure.

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

Nel rispetto dell'art.32 del Regolamento UE, con competenza sulle attività di ordinaria amministrazione e sulle attività dell'area Ricerca e con competenza sul Centro di Formazione, saranno date, nell'ambito dello specifico incarico, idonee istruzioni per mettere in atto tutte le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato, in esecuzione degli scopi statutari, con specifico riferimento al monitoraggio e segnalazione degli incidenti, degli eventi anomali e delle violazioni dei dati personali (data breach).

Si è proceduto analogamente all'adozione di modalità di ripristino della disponibilità dei dati e dell'accesso nei casi di incidente fisico o tecnico (perdita o furto). I medesimi Responsabili del Trattamento riceveranno istruzioni specifiche di adottare tutte le misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti; di informare il Titolare del trattamento e il DPO, senza ingiustificato ritardo, e comunque non oltre le 72 ore dal momento in cui se ne venga a conoscenza, di eventuali violazioni dei dati personali (data breach) adottando, di concerto con gli stessi, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente. Sarà richiesto, altresì, di predisporre e aggiornare un registro che dettagli, in caso di eventuali data breach, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate.

ATTIVITA' DI VERIFICA DEL POSSESSO DELLA CERTIFICAZIONE VERDE PER L'ACCESSO NEI LUOGHI DI LAVORO DELL'AZIENDA ai sensi del D.L. n. 127 – 21 settembre 2021

Ritenuta la straordinaria necessità e urgenza di integrare il quadro delle vigenti misure di contenimento della diffusione del virus SARS-CoV-2 il Governo, al fine di agevolare la graduale ripresa delle attività economiche e sociali, nel rispetto delle esigenze di contenimento della diffusione dell'epidemia da COVID-19, ha emanato decreto-legge n. 127/2021, volto a definire le modalità di controllo del possesso della Certificazione Verde (Green Pass o GP) da parte dei dipendenti del settore privato per l'accesso ai luoghi di lavoro, formazione o di volontariato a partire dal 15 ottobre 2021, fino alla cessazione dello stato di emergenza, attualmente fissato al 31 dicembre 2021.

Le attività di verifica del GP o della Certificazione medica di esenzione comportano, secondo le indicazioni del Garante della privacy, un trattamento di dati personali, che deve svolgersi ai sensi della normativa GDPR (Regolamento Europeo 2016/679) e secondo le modalità di cui al DPCM 17 giugno 2021.

Come precisato dal Garante privacy, il trattamento funzionale alla verifica del GP non necessita di alcuna autorizzazione da parte della stessa Autorità; inoltre, se condotto conformemente al DPCM 17 giugno 2021 e nel rispetto delle norme in materia di protezione dei dati personali (e in primo luogo del principio di minimizzazione dei dati conservati) non può determinare alcun illecito, né tantomeno l'irrogazione delle sanzioni da parte del Garante stesso.

In sede di verifica del GP o dell'esenzione, le informazioni oggetto di trattamento sono:

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

1. le generalità del lavoratore, nonché la validità, l'integrità e l'autenticità del certificato verde ovvero le predette informazioni in merito allo stato di soggetto esente da vaccinazione anti COVID-19;
2. le generalità del lavoratore e il mancato possesso del GP.

Il trattamento si concretizza nella consultazione/presa visione delle citate informazioni (analogamente alla presa visione della temperatura) e non è consentita, in alcun caso, come più volte ribadito, la raccolta dei dati dell'intestatario della certificazione in qualunque forma. Pertanto, ai fini dell'organizzazione dei controlli, non è possibile acquisire dal lavoratore, né preventivamente, né ex post, la certificazione in corso di validità ovvero dichiarazioni in ordine alla tipologia e alla scadenza della stessa.

Il Garante privacy ha annotato, infatti, che l'acquisizione di copia della certificazione verde e la registrazione della relativa scadenza, sebbene volte ad agevolare lo svolgimento dei controlli, siano in contrasto con gli obiettivi di bilanciamento tra privacy, tutela della salute e ripresa delle attività produttive in quanto rendono accessibili di dati personali superiori a quelli necessari. L'Authority mette in guardia dal rischio di rilevazione di dati eccedenti le finalità perseguite e, in particolare, di dati inerenti alla condizione sanitaria dell'interessato in banche date la cui sicurezza è da verificare.

Secondo il Garante tuttavia, in un'ottica organizzativa, non solo delle verifiche dei GP, ma più in generale dell'attività di impresa (es. gestione turni, trasferte, sostituzioni) sembrerebbe consentito al datore di lavoro di richiedere al lavoratore di comunicare preventivamente, con riferimento a uno specifico periodo di interesse (es. settimana/mensilità presa in considerazione per l'organizzazione ordinaria dei turni ovvero di una specifica trasferta ovvero di presenza necessaria in ragione della specificità della prestazione di uno specifico lavoratore), se non sarà in possesso della certificazione richiesta per l'accesso ai luoghi di lavoro.

In ragione di quanto in precedenza il Garante ritiene possibile che il Datore di lavoro possa richiedere, nell'ambito della procedura di verifica del possesso del GP, espressamente al lavoratore il possesso del GP riferito a un determinato periodo di interesse da individuarsi in relazione alle caratteristiche organizzative dell'impresa (es. settimana/mensilità presa in considerazione per l'organizzazione ordinaria dei turni ovvero di una specifica trasferta ovvero di presenza necessaria in ragione della specificità della prestazione di uno specifico lavoratore). Detta richiesta è legittimata, secondo il Garante, dall'art. 6, par. 1, lett. f) del Regolamento n. 2016/679 (GDPR) sul legittimo interesse del datore di lavoro di organizzare l'attività d'impresa, fermo il diritto dell'interessato di opporsi a tale trattamento.

Con riferimento a quanto rappresentato ISFORT disporrà, quando del caso, idonea comunicazione al lavoratore per accertare il possesso da parte del lavoratore di GP in un determinato periodo di interesse ai fini di attività specifiche di impresa fermo comunque l'obbligo del Datore di lavoro di effettuare i controlli delle Certificazioni prodotte dai lavoratori, nonché la possibilità del lavoratore di comunicare il mancato possesso del GP ovvero di non esibirlo al momento dell'accesso al luogo di lavoro.

A seguito di quanto disposto dal D.L. 127/2021 ISFORT ha provveduto a emanare:

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

- Protocollo per la verifica del possesso della certificazione verde per l'accesso nei luoghi di lavoro dell'azienda ai sensi del d.l. n. 127 – 21 settembre 2021;
- Comunicazione interna al Personale;
- Lettera di incarico all'Addetto alla Verifica del Green Pass AdT/VGP
- Istruzioni all'AdT/VGP
- Registro delle Verifiche del GP
- Verbale di constatazione di esito negativo della verifica del GP
- Comunicazione al Lavoratore in esito alla verifica del GP

Conseguentemente ISFORT ha disposto il presente aggiornamento del proprio DPIA e del Registro dei Trattamenti previsto a norma del Regolamento n. 2016/679 (GDPR).

4. Identificazione delle Risorse da Proteggere

Le risorse coinvolte nel trattamento dei dati personali sono state divise in alcune categorie:

- **Luoghi Fisici.** Sono stati analizzati tutti i luoghi ove fisicamente si svolge il trattamento dei dati o si trovano i sistemi di elaborazione o i luoghi ove si conservano i dati.
- **Risorse hardware.** Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Tra queste particolare rilievo hanno: il server della rete locale di Isfort, ove sono conservati i dati in formato elettronico, ed terminali da cui vengono eseguiti i programmi che elaborano i trattamenti.
- **Risorse dati.** Sono stati analizzati tutti gli archivi contenenti dati personali trattati dall'Istituto siano essi in formato elettronico che in formato cartaceo.
- **Risorse software.** Sono stati analizzati i software applicativi mediante i quali vengono effettuati i trattamenti automatizzati.

Si conferma quanto rappresentato in precedenza, ovvero che l'identificazione delle risorse da proteggere è stata effettuata con specifica attenzione ai luoghi fisici, le risorse hardware, dati e software che interessano la raccolta e trattamento dei dati personali nell'ambito delle attività di formazione regolata, erogata da Isfort, per il tramite del proprio CdF, come Centro di formazione riconosciuto da ANSF, Agenzia Nazionale per la Sicurezza delle Ferrovie, che consentono di organizzare corsi per il rilascio della Licenza europea per la condotta dei treni.

4.1 Luoghi Fisici.

Il luogo fisico in cui avvengono i trattamenti è la sede legale della Società, ubicata in Via Nizza, n. 45, 00198 Roma, ove avviene il trattamento diretto dei dati (raccolta, gestione, conservazione).

Nell'allegato 2 al DPIA, è evidenziata **la pianta dei locali** della sede, ai fini della identificazione degli uffici, degli archivi e dei terminali, ove sono svolte le diverse attività di trattamento dati con le indicazioni delle diverse forme di trattamento dati avuto riguardo della distinzione operata tra:

- **attività dell'area ricerca**, che non comportano trattamento di categorie particolari di dati e che, pertanto, **non richiedono** specifica valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA);
- **attività dell'area formazione regolata**, relativa ai corsi erogati dal Centro di formazione (CdF) riconosciuto da ANSF, Agenzia Nazionale per la Sicurezza delle Ferrovie, che **comportano l'effettuazione** della già citata valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA) in applicazione del disposto della sezione 3 e degli artt. 27 e 35 del Regolamento UE 2016/679 – GDPR, e costituiscono il principale argomento del presente documento.

Nel predisporre la presente DPIA si è ritenuto, in ogni caso, di rilevare tutti i luoghi fisici e tutte le risorse hardware dell'Istituto, anche in aree ove non avvengono trattamenti di categorie particolari di dati, al di là della distinzione in precedenza rappresentata tra i trattamenti effettuati in azienda,

In alcune stanze individuali e in quelle a uso promiscuo le categorie particolari di dati **sono trattate esclusivamente da persone delegate dal TdT**, con specifico provvedimento di delega *ad personam*. Le attività di trattamento di categorie particolari di dati, come in precedenza detto, sono esclusivamente **le attività dell'area formazione regolata**, relativa ai corsi erogati dal Centro di formazione (CdF) riconosciuto da ANSF, Agenzia Nazionale per la Sicurezza delle Ferrovie.

Per il **trattamento dei dati nell'area formazione regolata** Isfort ha scelto di effettuare la gestione, pubblicazione, archiviazione e backup dei **dati attraverso il servizio di file hosting Dropbox**, che offre un'area di lavoro in team per la condivisione di strumenti di lavoro, creazione di contenuti e archiviazione protetta, in linea con le politiche predefinite e autorizzate dal TdT.

A tale riguardo è stata attivato un contratto Dropbox Business che consente di operare sulla piattaforma cloud con 4 licenze di accesso, **attraverso login e password abilitate da persona all'uopo incaricata** da parte del TdT.

Possono accedere alla piattaforma, **anche da remoto, esclusivamente le persone delegate dal TdT**, che svolgono attività di trattamento dati nell'area formazione regolata, con **PC protetti da login e password**. Attraverso la doppia procedura di autenticazione, si realizza **una doppia protezione di sicurezza** delle categorie particolari di dati.

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

Per quanto attiene alla sicurezza della piattaforma Dropbox, si rinvia alle specifiche di sistema rese note dalla società proprietaria del prodotto indicate sul sito www.dropbox.com/it/business, precisando che il sistema si basa sul protocollo crittografico Secure Sockets Layer (SSL) e che i files immagazzinati e accessibili tramite login e password vengono cifrati tramite AES con chiave a 256 bit. Dropbox garantisce, nelle sue specifiche di privacy, la continua verifica dei propri standard di sicurezza secondo le norme ISO e assicura, nel contempo che i suoi interventi di gestione del sistema sono volti solo al miglioramento dell'architettura software escludendo categoricamente intromissioni sui files archiviati dai clienti.

Si conferma, inoltre, che in alcune stanze della sede non sono effettuati trattamenti di categorie particolari di dati e non sono gestiti e archiviati documenti relativi a trattamenti di dati di natura personale.

Per quanto attiene ai dati personali dei soggetti interessati trattati presso le società consulenti, in relazione agli incarichi conferiti, si rimanda alle specifiche misure adottate dalle predette entità, dalle quali si è ottenuta specifica dichiarazione di osservanza delle norme del Regolamento UE 2016/679 – GDPR .

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE LUOGHI FISICI N. 01

Città:	ROMA
Indirizzo Sede:	Via Nizza, n. 45, Roma, scala B interno 7 secondo piano

Locali			
Descrizione e posizione	Uso	Dispositivo di protezione dell'accesso ai locali: porta blindata con chiave anti duplicazione (duplicazione consentita solo con scheda di tipo smart card)	Note
<u>Stanza 1</u>	Ufficio TdT/RdT/IS	In questa stanza non sono presenti gli archivi contenenti documenti di natura cartacea contenenti categorie particolari di dati. Il trattamento di dati sensibili a mezzo PC è effettuato da persona autorizzata: Marco Romani, n.q. TdT/RdT/IS. Il TdT non dispone di licenza di accesso a Dropbox.	I dati sul pc sono protetti da password. Questa stanza viene utilizzata in maniera promiscua. I documenti cartacei non appena termina l'eventuale trattamento vengono immediatamente riportati negli archivi di competenza (Stanza 7/A). Autorizzati ad accedere al PC n.1: Marco Romani n.q. TdT
<u>Stanza 2</u>	Ufficio operativo IS	In questa stanza non vengono effettuati trattamenti di categorie particolari di dati e non sono presenti archivi di natura cartacea relativi ai predetti dati	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave e i dati sul pc sono protetti da password. Autorizzati ad accedere al PC n. 2: Carlo Carminucci n.q. Dir. Ricerca e RDQ
<u>Stanza 3</u>	Ufficio operativo IS	In questa stanza non sono presenti gli archivi di documenti di natura cartacea contenenti categorie particolari di dati. Il trattamento di dati sensibili a mezzo PC è effettuato da persona incaricata : Massimo Procopio, n.q. RSI. Il TdT non dispone di licenza di accesso a Dropbox.	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave e i dati sul pc sono protetti da password. Autorizzati ad accedere: al PC n. 3: Daniela Campora n.q. Amministrazione e AdT/IS; al PC n. 4: Massimo Procopio n.q. RSI; al PC n. 5: Luca Trepiedi n.q. ricercatore

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

<u>Stanza 4</u>	Ufficio operativo IS	In questa stanza non sono presenti gli archivi di documenti di natura cartacea contenenti categorie particolari di dati. Il trattamento di dati sensibili a mezzo PC è effettuato da persona incaricata : Angela Chindemi, n.q. Resp. Ufficio Analisi e Metodologia Statistica.	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave e i dati sul pc sono protetti da password. Autorizzati ad accedere: al PC n. 6 Angela Chindemi n.q. Resp. A. e M. Statistica; al PC n. 8: Ricercatore; al PC. N. 9: /;
<u>Stanza 5</u>	Stanza server	In questa stanza non sono presenti gli archivi di documenti di natura cartacea contenenti categorie particolari di dati. Il trattamento di dati sensibili a mezzo PC è effettuato da persona incaricata : Massimo Procopio, n.q. RSI	La stanza è protetta da porta chiusa a chiave e i dati sul pc sono protetti da password. Autorizzati ad accedere al PC n. 10: Massimo Procopio n.q. RSI
<u>Stanza 6</u>	Ufficio operativo IS	In questa stanza non vengono effettuati trattamenti di categorie particolari di dati e non sono presenti archivi di natura cartacea relativi ai predetti dati	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave, e i dati sul pc sono protetti da password. Autorizzati ad accedere al PC n. 11:Marco Milli n.q. Presidente; PC n. 7 Marina Ferrara ricercatore
<u>Stanza 7</u>	Ufficio operativo IS	In questa stanza non sono presenti gli archivi di documenti di natura cartacea contenenti categorie particolari di dati. Il trattamento di dati sensibili a mezzo PC è effettuato da persone incaricate. Autorizzati con licenza di accesso Dropbox: Cesare Borgia n.q. RdT/CdF; Paolo Paccosi n.q. AdT/CdF/RQ; persone diverse, di volta in volta nominate, n.q. AdT/CdF/NIPI, di volta in volta abilitati con licenza di accesso a Dropbox. Al momento questa licenza è assegnata a Valerio Tiberi, Istruttore n.q. AdT/CF/NIPI	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave e i dati sul pc sono protetti da password. Autorizzati ad accedere: al PC n.12 Vincenzo Saccà n.q. SVI/RE/RI; al PC n.13 Paolo Paccosi n.q. AdT/CdF/RQ e Giulia Carbone n.q. ricercatore; al PC n. 17 Cesare Borgia n.q. RdT/CdF; al PC n. 18 persone diverse di volta in volta autorizzate, n.q. AdT/CF/NIPI;
<u>Stanza 7/A</u>	Ufficio operativo IS	In questa stanza sono presenti gli archivi di documenti di natura cartacea contenenti categorie particolari di dati, conservati in armadi chiusi a chiave. L'accesso a detti archivi è consentito solo alle persone incaricate, con obbligo di	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

		trattenere i documenti per il tempo necessario al trattamento (consultazione, aggiornamento etc) e obbligo di riconsegna non appena terminato detto uso.	
<u>Stanza 8</u>	Ufficio operativo	In questa stanza non sono presenti gli archivi di documenti di natura cartacea contenenti categorie particolari di dati. Il trattamento di dati sensibili a mezzo PC è effettuato da persona incaricata, Angela Cesaroni, abilitata con licenza di accesso Dropbox, anche con compiti di amministratore degli accessi Dropbox, n.q. AdT/IS e AdT/CF/NIPS	L'accesso e l'uso della stanza è promiscuo. I dati sul pc sono protetti da password. Autorizzati ad accedere al PC 14: Angela Cesaroni n.q. AdT/IS e AdT/CF/NIPS
<u>Stanza 9</u>	Ufficio operativo IS	In questa stanza non vengono effettuati trattamenti di categorie particolari di dati e non sono presenti archivi di natura cartacea relativi ai predetti dati	L'accesso e l'uso della stanza è promiscuo. La stanza è protetta da porta chiusa a chiave e i dati sul pc sono protetti da password. Autorizzati ad accedere: al PC n. 15 Andrea Appetecchia n.q. ricercatore; al PC n. 16 Dayana Bou Shakra n.q. ricercatore

4.2 Risorse Hardware.

Nel predisporre la presente DPIA si è ritenuto, in ogni caso, di rilevare tutte le risorse hardware dell'Istituto, al di là della distinzione in precedenza rappresentata tra i trattamenti effettuati in azienda, nell'area ricerca e nell'area formazione delegata ANSF.

Le risorse hardware utilizzate per trattare i dati identificativi personali di natura sensibile (PC e Server) sono analizzate nelle seguenti schede riepilogative, in cui sono identificate anche le persone all'uopo **specificamente delegate da parte del TdT**. Si ricorda che il trattamento dei dati può avvenire anche utilizzando i notebook dell'Istituto, ma con l'obbligo di cancellare o copiare il tutto nelle cartelle condivise salvate tramite server su Dropbox, come illustrato in precedenza. Non è consentito lasciare alcun dato dell'Istituto sugli stessi notebook.

Come anzi detto si sono rilevate anche le risorse hardware utilizzate in aree aziendali ove non sono trattate categorie particolari di dati.

Nell'allegato n. 3 è descritta l'architettura di rete interna collegata al server ubicato in stanza n. 5.

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 01

Codice:	PC N.1 in uso a Marco Romani n.q. TdT
Descrizione:	PC N.1
Modello:	Intel Core I5-9400 cpu 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 1 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note: L'utente abilitato ad accedere e a cambiare password e la User ID è l'RSI (indicato nei mansionari privacy)
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione <small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 02

Codice:	PC N.2 in uso a Carlo Carminucci n.q. Direttore Ricerca e RDQ
Descrizione:	PC N.2
Modello:	Intel Core i5-9400 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 2 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note: L'utente abilitato ad accedere e a cambiare password e la User ID è l'RSI (indicato nei mansionari privacy)
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 03

Codice:	PC N.3 in uso a Daniela Campora n.q. Amministrazione e AdT/IS
Descrizione:	PC N.3
Modello:	Intel Core i5-7400 CPU 3.00GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 3 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input type="checkbox"/> L'utente può cambiare autonomamente la password di accesso al dominio Note: L'utente abilitato ad accedere e a cambiare password e la User ID è l'RSI (indicato nei mansionari privacy)
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	Il backup viene effettuato automaticamente con cadenza giornaliera sul server.

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 04

Codice:	PC N.4 in uso a Massimo Procopio n.q. RSI
Descrizione:	PC N.4
Modello:	Intel Core i7-8700 CPU 3.20 GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 3 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione (nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 05

Codice:	PC N.5 in uso a LucaTrepiedi n.q. ricercatore
Descrizione:	PC N.5
Modello:	ADM Phenom II X2 B55 Processor 3.00GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 3 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione (nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 06

Codice:	PC N.6 in uso a Angela Antonia Chindemi n.q. Resp.Analisi Metodologia Statistica
Descrizione:	PC N.6
Modello:	Intel Core i9-10900X CPU 3.70GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 4 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input type="checkbox"/> L'utente può cambiare autonomamente la password Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione (nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEMA RILEVAZIONE RISORSE HARDWARE N. 07

Codice:	PC N.7 in uso a Marina Ferrara n.q. ricercatore
Descrizione:	PC N.7
Modello:	Intel Core i7-10700 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 6 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input type="checkbox"/> L'utente può cambiare autonomamente la password Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione <small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 08

Codice:	PC N. 8 in uso a Ricercatore
Descrizione:	PC N.8
Modello:	Intel Core i7-10700 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 4 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input type="checkbox"/> L'utente può cambiare autonomamente la password Note:
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione <small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 09

Codice:	PC N. 9
Descrizione:	PC N. 9
Modello:	Intel Core i7-10700 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 4 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione <small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 10

Codice:	PC N.10 Server in uso a Massimo Procopio n.q. RSI
Descrizione:	Server
Modello:	Intel Xeon CPU 3.06GHz (2 procesori)
Sistema Operativo:	Windows Server Standard
Categoria:	Sistema Elaborativo Server
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 5 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione (nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 11

Codice:	PC N.11 in uso a Marco Milli n.q. Presidente
Descrizione:	PC N.11
Modello:	Pentium Dual Core CPU E5800 3.20GHz
Sistema Operativo:	Windows 7 Professional
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 6 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione <small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 12

Codice:	PC N.12 in uso a Vincenzo Saccà n.q. SVI/RE/RI
Descrizione:	PC N.12
Modello:	Intel Core i5-4460 CPU 3.20GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 7 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione <small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 13

Codice:	PC N.13 in uso a Paolo Paccosi n.q. AdT/CdF/RQ e Giulia Carbone n.q. ricercatore
Descrizione:	PC N.13
Modello:	Pentium Dual Core CPU E5400 2.70GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 7 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note:
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	<small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDE RILEVAZIONE RISORSE HARDWARE N. 14

Codice:	PC n. 14 in uso a Angela Cesaroni n.q. AdT/IS e AdT/Cdf/NIPS
Descrizione:	PC n. 14
Modello:	Intel Core i5-9400 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 8 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input type="checkbox"/> L'utente può cambiare autonomamente la password di accesso al dominio Note: L'utente abilitato ad accedere e a cambiare password e la User ID è l'RSI (indicato nei mansionari privacy)
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Descrizione il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	<small>(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)</small>
Unità di backup	Il backup viene effettuato automaticamente con cadenza giornaliera sul server.

**Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.**

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 15

Codice:	PC N.15 in uso a Andrea Appetecchia n.q. ricercatore
Descrizione:	PC N.15
Modello:	Intel Core i5-9400 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	[] No [X] Rete Privata [] Rete Disponibile al pubblico;
Dislocazione:	Stanza 9 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	[] No [X] Si [] L'utente può cambiare autonomamente la password Note: L'utente abilitato ad accedere e a cambiare password e la User ID è l'RSI (indicato nei mansionari privacy)
Antivirus:	[] No [X] Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	[] No [X] Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

Istituto Superiore di Formazione e Ricerca per i Trasporti
ISFORT S.P.A.

Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 16

Codice:	PC N.16 in uso a Dayana Bou Shakra n.q. ricercatore
Descrizione:	PC N.16
Modello:	Intel Core i7-10700 CPU 2.90GHz
Sistema Operativo:	Windows 10 Pro
Categoria:	Sistema Elaborativo Client
Elaboratore in rete:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 9 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input type="checkbox"/> L'utente può cambiare autonomamente la password Note: L'utente abilitato ad accedere e a cambiare password e la User ID è l'RSI (indicato nei mansionari privacy)
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Descrizione: il server è protetto da gruppo di continuità per impedire che improvvise cadute di tensione danneggino i dati sopra conservati.

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 17

Codice:	PC n.17 in uso a Cesare Borgia n.q. RdT/CdF
Descrizione:	PC n.17
Modello:	Produttore: Notebook Acer equipaggiato con Intel i5, 8Gb Ram
Sistema Operativo:	Windows 10 Pro
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	stanza 7

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input checked="" type="checkbox"/> L'utente può cambiare autonomamente la password di accesso al dominio
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Si Descrizione

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	I backup vengono effettuati periodicamente con cadenza settimanale in maniera automatica sul server

ISFORT S.P.A.
 Istituto Superiore di Formazione e Ricerca per i Trasporti
 Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE HARDWARE N. 18

Codice:	PC n.18 in uso a Istruttori /Esaminatori n.q. AdT/CF/NIPI
Descrizione:	PC n.18
Modello:	Produttore: Notebook Lenovo Intel i3, 4Gb DDR4 Ram
Sistema Operativo:	Windows 10 Pro
Categoria:	<input type="checkbox"/> Sistema Elaborativo Server <input checked="" type="checkbox"/> Sistema Elaborativo Client <input type="checkbox"/> Altro Sistema:
Elaboratore in rete:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Rete Privata <input type="checkbox"/> Rete Disponibile al pubblico;
Dislocazione:	Stanza 7 (Vedere allegato 1 al DPIA)

DISPOSITIVI DI PROTEZIONE

Presenza di Password e User ID:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si <input checked="" type="checkbox"/> L'utente può cambiare autonomamente la password di accesso al dominio
Antivirus:	<input type="checkbox"/> No <input checked="" type="checkbox"/> Si Tipo/Prodotto: Eset NOD32 Antivirus Periodicità di aggiornamento: L'archivio contenete le firme dei virus è aggiornato automaticamente quando rileva le nuove definizioni.
Altri dispositivi:	<input checked="" type="checkbox"/> No <input type="checkbox"/> Si Descrizione

COMPONENTI DI RILIEVO AI FINI DELLA SICUREZZA DEI DATI

Componente	Descrizione
	(nel caso in cui si tratti di un dispositivo di memorizzazione indicare se ospita una risorsa dati)
Unità di backup	-

4.3 Risorse dati.

Gli archivi e le banche dati trattate, contenenti categorie particolari di dati personali, relativamente all'area CdF, formazione regolata ANSF, sono le seguenti:

- BANCA DATI partecipanti al corso n. 1 **Arch. N.1**
- BANCA DATI ORGANI SOCIALI **Arch. N. 2**
- ARCHIVIO CORRISPONDENZA **Arch. N. 3**

SCHEDA RILEVAZIONE RISORSE DATI N. 01

Codice:	<ul style="list-style-type: none"> • BANCA DATI partecipanti ai corsi per l'acquisizione della Licenza EU Archivio n.1
Descrizione:	Banca dati partecipanti ai corsi di formazione regolata ANSF per il conseguimento di Licenza EU. Sono trattati e archiviati, pertanto, dati anche di categorie particolari, relativi ai partecipanti ai corsi. I dati sono raccolti per fini gestionali dell'Istituto e strettamente necessari al conseguimento della licenza. I dati sono esclusivamente identificativi personali, alcuni rientranti tra le categorie particolari di dati (idoneità, qualificazione, etc) e altri non sensibili quali i dati anagrafici.
Tipologia risorsa:	<input checked="" type="checkbox"/> Archivio Elettronico <input checked="" type="checkbox"/> Archivio cartaceo L'archivio cartaceo è conservato secondo le seguenti modalità: Dati identificativi personali partecipanti/ (Ufficio "Stanza 7/A" – Arch.1.) I dati conservati in detto archivio sono rimossi se la rimozione è richiesta dall'interessato, a norma del Regolamento UE 2016/679 oppure dalla società entro il termine di 5 anni. La medesima banca dati è conservata anche in formato elettronico su Dropbox con accessi controllati a persone autorizzate dal TdT che accedono con login e password autorizzate, come descritto in precedenza.
Risorse Hardware su cui è ospitata: <small>(solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)</small>	Le persone autorizzate ad accedere all'archivio elettronico su Dropbox, descritto in precedenza, utilizzano i pc descritti nelle schede 13,17 e 18, ubicati in stanza 7 e il pc 14 ubicato in stanza 8. Da tenere in conto, come detto più sopra, che l'archivio elettronico n.1 è posizionato su Dropbox e, pertanto, come autorizzato dal TdT, è accessibile dagli autorizzati anche in remoto, con PC portatili, che accedono con login e password autorizzate, come descritto in precedenza.

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO

Dato	Natura del dato
Dati di partecipazione al corso	Dato sensibile
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo	Dato non sensibile
Attività economiche, commerciali, finanziarie, etc.	Dato non sensibile

STRUMENTI E POLITICHE DI BACKUP

ISFORT S.P.A.
Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

Dispositivo di backup:	<input checked="" type="checkbox"/> Non esistente in rete locale <input type="checkbox"/> Essendo l'archivio 1 posizionato su Dropbox il backup avviene con procedure dettate dal sistema.
Incaricati del backup:	Il backup viene attivato da persona incaricata p.t., Angela Cesaroni, abilitata con licenza di accesso Dropbox, anche con compiti di amministratore degli accessi Dropbox, n.q. AdT/CF/NIPS

Supporti di backup:	Essendo l'archivio 1 posizionato su Dropbox le modalità e tempistiche di backup sono prescritte dal sistema.
----------------------------	--

SCHEDA RILEVAZIONE RISORSE DATI N. 2

4

Codice:	DATI ORGANI SOCIALI
Descrizione:	BANCA DATI ORGANI SOCIALI . In questa banca dati sono conservati i dati dei MEMBRI DEGLI Organi Sociali di Isfort. I dati sono raccolti per fini di corretta gestione amministrativa e segretariale. I dati sono esclusivamente identificativi personali e non sensibili. Qualora fossero trattati dati sensibili si provvederà secondo la norma.
Tipologia risorsa:	[X] Archivio Elettronico [X] Archivio cartaceo Nota: parte dei dati sono in formato cartaceo. Questi sono conservati secondo le seguenti modalità: Dati identificativi personali : ORGANI SOCIALI (Ufficio Stanza 3 – arch. 2)
Risorse Hardware su cui è ospitata: (solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)	SERVER ubicato nella stanza n. 5

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO

Dato	Natura del dato
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo	Dato non sensibile
Attività economiche, commerciali, finanziarie, etc.	Dato non sensibile

5 STRUMENTI E POLITICHE DI BACKUP

Dispositivo di backup:	[X] Non esistente [...]
Incaricati del backup:	N.A.
Supporti di backup:	N.A.

SCHEDA RILEVAZIONE RISORSE DATI N. 3

Codice:	CORRISPONDENZA DATI IN TRATTAMENTO
Descrizione:	BANCA DATI CORRISPONDENZA. In questa banca dati è raccolta la corrispondenza della Organizzazione relativa al trattamento dati sensibili dell'area CdF ovvero partecipanti ai corsi di formazione regolata ANSF per il conseguimento di Licenza EU. Sono trattati e archiviati, pertanto, corrispondenza relativa anche a categorie particolari di dati. I dati sono raccolti per fini gestionali dell'Istituto, per tenere i contatti con i partecipanti o perché strettamente necessari al conseguimento della licenza. I dati sono esclusivamente identificativi personali, alcuni rientranti tra le categorie particolari di dati (idoneità, qualificazione, etc) e altri non sensibili quali i dati anagrafici.
Tipologia risorsa:	<input checked="" type="checkbox"/> Archivio Elettronico <input checked="" type="checkbox"/> Archivio cartaceo La banca dati n. 3 è conservata anche in formato elettronico su Dropbox con accessi controllati a persone autorizzate dal TdT che accedono con login e password autorizzate, come descritto in precedenza. Parte dei dati sono in formato cartaceo. Questi sono conservati secondo le seguenti modalità: Dati identificativi personali dei soggetti con cui l'Istituto intrattiene corrispondenza in armadio chiuso a chiave conservato nella stanza 7/A.
Risorse Hardware su cui è ospitata: <small>(solo per archivi elettronici; eventualmente fare riferimento alla scheda rilevazione risorse hardware)</small>	Le persone autorizzate ad accedere all'archivio elettronico della banca dati n. 3, posizionata su Dropbox, come descritto in precedenza, utilizzano i pc descritti nelle schede 13,17 e 18, ubicati in stanza 7 e il pc 14 ubicato in stanza 8. Da tenere in conto, come detto più sopra, che l'archivio elettronico n.3 è posizionato su Dropbox e, pertanto, come autorizzato dal TdT, è accessibile dagli autorizzati anche in remoto, con PC portatili, che accedono con login e password autorizzate, come descritto in precedenza.

NATURA DEI DATI PERSONALI PRESENTI SULL'ARCHIVIO

Dato	Natura del dato
Codice Fiscale ed altri dati di identificazione personale, nominativo, indirizzo	Dato non sensibile
Dati sensibili per caratteristiche partecipante ai corsi	Dato sensibile

STRUMENTI E POLITICHE DI BACKUP

Dispositivo di backup	<input checked="" type="checkbox"/> Non esistente in rete locale <input type="checkbox"/> Essendo l'archivio 3 posizionato su Dropbox il backup avviene con
------------------------------	---

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

procedure dettate dal sistema.

Il backup viene attivato da persona incaricata p.t., Angela Cesaroni, abilitata con licenza di accesso Dropbox, anche con compiti di amministratore degli accessi Dropbox, n.q. AdT/CF/NIPS con le modalità e tempistiche di backup prescritte dal sistema.

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

4.4 Risorse software

Le risorse software utilizzate nel trattamento dei dati personali sono analizzate nelle seguenti schede riepilogative:

ISFORT S.P.A.
 Istituto Superiore di Formazione e Ricerca per i Trasporti
 Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE SOFTWARE N. 01

Codice:	SW01
Descrizione:	WINDOWS 10
Produttore:	MICROSOFT
Risorse Hardware su cui può essere eseguito: (eventualmente fare riferimento alla scheda rilevazione risorse hardware)	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati (eventualmente fare riferimento alla scheda rilevazione risorse dati)	Annotazioni
Tutte	

ISFORT S.P.A.
 Istituto Superiore di Formazione e Ricerca per i Trasporti
 Via Nizza, 45 00198 ROMA

SCHEMA RILEVAZIONE RISORSE SOFTWARE N. 02

Codice:	SW02
Descrizione:	OFFICE 2010 PROFESSIONAL
Produttore:	MICROSOFT
Risorse Hardware su cui può essere eseguito: <small>(eventualmente fare riferimento alla scheda rilevazione risorse hardware)</small>	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati <small>(eventualmente fare riferimento alla scheda rilevazione risorse dati)</small>	Annotazioni
Dati Clienti	Base Dati ad uso esclusivamente interno.

ISFORT S.P.A.
Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE SOFTWARE N. 03

Codice:	SW03
Descrizione:	ADOBE ACROBAT
Produttore:	ADOBE SYSTEMS
Risorse Hardware su cui può essere eseguito: (eventualmente fare riferimento alla scheda rilevazione risorse hardware)	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati (eventualmente fare riferimento alla scheda rilevazione risorse dati)	Annotazioni
Dati Clienti	Base Dati ad uso esclusivamente interno.

ISFORT S.P.A.
Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE SOFTWARE N. 04

Codice:	SW04
Descrizione:	EDGE
Produttore:	MICROSOFT
Risorse Hardware su cui può essere eseguito: (eventualmente fare riferimento alla scheda rilevazione risorse hardware)	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati (eventualmente fare riferimento alla scheda rilevazione risorse dati)	Annotazioni
Dati Clienti	

ISFORT S.P.A.
 Istituto Superiore di Formazione e Ricerca per i Trasporti
 Via Nizza, 45 00198 ROMA

SCHEDA RILEVAZIONE RISORSE SOFTWARE N. 05

Codice:	SW05
Descrizione:	CHROME
Produttore:	GOOGLE
Risorse Hardware su cui può essere eseguito: <small>(eventualmente fare riferimento alla scheda rilevazione risorse hardware)</small>	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati <small>(eventualmente fare riferimento alla scheda rilevazione risorse dati)</small>	Annotazioni
Dati Clienti	

ISFORT S.P.A.
Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

SCHEMA RILEVAZIONE RISORSE SOFTWARE N. 06

Codice:	SW06
Descrizione:	MOZILLA FIREFOX
Produttore:	MOZILLA FOUNDATION
Risorse Hardware su cui può essere eseguito: (eventualmente fare riferimento alla scheda rilevazione risorse hardware)	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati (eventualmente fare riferimento alla scheda rilevazione risorse dati)	Annotazioni
Dati Clienti	

ISFORT S.P.A.
 Istituto Superiore di Formazione e Ricerca per i Trasporti
 Via Nizza, 45 00198 ROMA

SCHEMA RILEVAZIONE RISORSE SOFTWARE N. 07

Codice:	SW07
Descrizione:	DIKE GOSIGN
Produttore:	INFOCERT
Risorse Hardware su cui può essere eseguito: (eventualmente fare riferimento alla scheda rilevazione risorse hardware)	Tutte

BASI DATI SU CUI OPERA IL SOFTWARE

Base Dati (eventualmente fare riferimento alla scheda rilevazione risorse dati)	Annotazioni
Dati Clienti	Base Dati ad uso esclusivamente interno.

5. Analisi dei Rischi

5.1 ANALISI DEI RISCHI SUI LUOGHI FISICI

Risorsa <i>(tutte o una specifica)</i>	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
tutte	Possibilità di intrusione	Bassa	Porta blindata con sistema anti duplicazione della chiave (smart card)
tutte	Allagamenti	Bassa	Area non soggetta ad inondazioni o calamità di questo tipo.
tutte	Incendio	Bassa	Estintori a idrocarburi alogenati.
tutte	furto	Bassa	Porta blindata
tutte	Impossibilità di rilevare accessi non autorizzati	Bassa	I locali hanno un solo accesso sempre presidiato durante il normale svolgimento dell'attività lavorativa. Durante la chiusura degli uffici la porta blindata viene chiusa regolarmente.

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

5.2 ANALISI DEI RISCHI SULLE RISORSE HARDWARE

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
tutte	uso non autorizzato dell'hardware	Bassa	L'utilizzo dell'hardware in tutte le aree è soggetto all'utilizzo di password
tutte	Manomissione/sabotaggio	Bassa	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da società terze con supervisione dell'RSI.
tutte	Probabilità/frequenza di guasto	Bassa	L'hardware acquistato è di qualità e storicamente non ha mai dato problemi rilevanti.
tutte	Intercettazione delle trasmissioni	Media	Il router è collegato a linee ADSL.
tutte	Rischi connessi all'elettricità.	Alta	Non sono previsti gruppi di continuità per l'hardware aziendale

5.3 ANALISI DEI RISCHI SULLE RISORSE DATI

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
tutte	accesso non autorizzato	Bassa	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password. All'archivio cartaceo possono accedere solo i diretti incaricati, in quanto gli archivi sono vigilati dal personale preposto a tale servizio.
tutte	Cancellazione non autorizzata di dati/manomissione di dati	Bassa	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password. All'archivio cartaceo possono accedere solo i diretti incaricati, in quanto gli archivi sono vigilati dal personale preposto a tale servizio.
tutte	Perdita di dati	Bassa	I dati non sensibili Isfort sono conservati su dischi standard. Vengono effettuate con cadenza varia copie di backup su hard disk secondari, pc in rete e su hard disk esterno USB. Le categorie particolari di dati trattate nell'area CdF sono a basso rischio di perdita in quanto salvati direttamente sul sistema Dropbox.
tutte	Incapacità di ripristinare copie di backup	Bassa	I controlli periodici effettuati sui supporti di backup hanno sempre fornito esiti positivi. Analogo discorso per i

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

			dati sensibili su Dropbox che garantisce la possibilità di ripristinare copie di backup.
--	--	--	---

5.4 ANALISI DEI RISCHI SULLE RISORSE SOFTWARE

Risorsa (tutte o una specifica)	Elemento di Rischio	Soglia Individuata	Eventuale Motivazione
tutte	Accesso non autorizzato alle basi dati connesse	Bassa	I sistemi operativi che trattano i dati controllano l'accesso tramite una finestra di autenticazione (finestra di Login).
tutte	Errori software che minacciano l'integrità dei dati	Bassa	I sistemi operativi sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati. Analogo discorso per i dati sensibili su Dropbox che garantisce la protezione da errori software che minacciano l'integrità dei dati.
tutte	Presenza di codice non conforme alle specifiche del programma	Bassa	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni. Analogo discorso per i dati sensibili su Dropbox che garantisce il continuo controllo sui propri codici conformi alle specifiche.

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

6. Definizione ed attuazione della Politica di Sicurezza

Al fine di assicurare l'integrità dei dati trattati ed impedirne la comunicazione e/o diffusione non autorizzata, la nostra Organizzazione ha elaborato una precisa Politica di Sicurezza basata sull'adozione di misure di tipo fisico, logico ed organizzativo. Tali misure avranno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal Regolamento UE 2016/679 sia un livello idoneo di sicurezza relativamente alle tipologie dei nostri dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

6.1 MISURE DI SICUREZZA ADOTTATE DI TIPO FISICO

Descrizione misura	Note ed indicazioni per la corretta applicazione
creazione di archivio ad accesso controllato/selezionato	<p>L'accesso all'appartamento è protetto da porta blindata.</p> <p>Gli archivi delle categorie particolari di dati trattati nell'area CdF su supporto cartaceo sono posizionati nella stanza 7/A, utilizzando degli armadi aventi una sezione a scaffali (per i supporti contenenti dati comuni) ed una munita di sportelli con serratura (per i supporti contenenti categorie particolari di dati personali).</p> <p>Gli incaricati al trattamento di tali dati potranno prelevare i documenti necessari per il trattamento per il tempo necessario a tale operazione, dopo di che avranno il compito di riportarli nel sopraccitato luogo preposto alla loro conservazione, sotto la supervisione degli incaricati alla custodia dell'archivio. Sarà compito dell'incaricato che preleva i documenti garantire che questi siano rinchiusi, sotto chiave, in un cassetto della propria scrivania nel periodo di temporanea assenza dal posto di lavoro.</p>
registrazione degli accessi	Nessuno accede alla sede aziendale fuori orario. Nel caso di necessità verranno identificati e registrati tutti coloro che consulteranno i dati fuori dall'orario stabilito;
autenticazione degli accessi	La vigilanza degli archivi delle categorie particolari di dati trattati nell'area CdF è stata affidata ad un rispettivo impiegato mediante lettera di incarico;
custodia in classificatori e armadi non accessibili	Per i documenti contenenti dati personali verranno utilizzati dei classificatori che saranno poi posizionati in armadi muniti di serratura;
vigilanza della sede	Fuori degli orari di ufficio il portone è chiuso e gli accessi avvengono con chiave.
sistemi di allarme e antincendio	<p>Sono presenti i seguenti sistemi di sicurezza:</p> <p>Estintori da Kg. 5 contenenti "idrocarburi alogenati" revisionati ogni 6 mesi;</p>

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

continuità elettrica alimentazione	I PC della sede non sono dotati di gruppi di continuità che garantiscono una stabilizzazione dell'energia elettrica erogata. Tali gruppi, in conseguenza di un improvvisa assenza di energia, garantiscono un'autonomia temporale necessaria a effettuare il salvataggio delle operazioni in corso e avviare le corrette procedure di spegnimento dell'elaboratore. L'organizzazione disporrà un programma di soluzione di detta criticità.
ingresso controllato	L'accesso agli uffici è vigilato dagli impiegati nelle ore di lavoro; non è consentito il libero accesso al pubblico.

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

6.2 MISURE DI SICUREZZA ADOTTATE DI TIPO LOGICO

Descrizione misura	Note ed indicazioni per la corretta applicazione
identificazione degli incaricati preposti alle attività relative al trattamento	Sono stati individuati e nominati per iscritto gli incaricati preposti alla custodia degli archivi e al trattamento delle categorie particolari di dati dell'area CdF. Agli incaricati, congiuntamente alla lettera di nomina, verranno indicate le norme operative e di sicurezza a cui attenersi. Le lettere di nomina sono presenti nei Mansionari DPIA.
assegnazione ed autorizzazione all'accesso su cui effettuare i trattamenti	A tutto il personale Isfort che utilizza le postazioni è stato assegnato un elaboratore tramite il quale potranno accedere agli archivi in formato elettronico su cui operare i trattamenti. Agli incaricati preposti alla custodia degli archivi e al trattamento delle categorie particolari di dati dell'area CdF sono state attribuite licenze di accesso al sistema Dropbox, protetti da login e password.
indicazione del custode delle password	La gestione delle licenze è affidata pro tempore a Angela Cesaroni n.q. addetto trattamento dati Centro di Formazione (AdT/CdF/NIPS), nominata per iscritto, dal TdT, custode delle licenze Dropbox che consentono l'accesso e il trattamento di categorie particolari di dati dell'area CdF. La lettera di nomina è presente nei Mansionari DPIA.
indicazione dell'amministratore di sistema	E' stato individuato e nominato per iscritto, dal TdT, l'amministratore di sistema RSI a cui è stato affidato il compito di sovrintendere alle risorse dei sistemi operativi degli elaboratori e delle basi dati ISF; sarà compito del RSI, su indicazione del TdT, disattivare i codici identificativi in caso di mancato utilizzo per un periodo superiore ai sei mesi. Lo stesso RSI potrà, su disposizione del TdT, avere accesso al sistema Dropbox, ove questo si rendesse necessario. La lettera di nomina dell'amministratore di sistema è presente nei Mansionari Privacy.
identificazione dell'incaricato/utente che accede ai dati dal terminale	E' stato attribuito un codice identificativo univoco (USER ID) a ciascun incaricato/utente Isfort per accedere al terminale assegnatogli. Tale codice sarà disattivato nel caso l'incaricato/utente perda la qualità che consentiva l'accesso al terminale o quando tale codice sia rimasto inutilizzato per un periodo superiore ai sei mesi. Analoga verifica periodica dell'utilizzo delle licenze Dropbox è effettuata dall'AdT/CdF/NIPS nell'ambito delle sue competenze.

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

autenticazione incaricato/utente	Possono accedere ai terminali Isfort solo coloro che sono autorizzati dal TdT e abilitati dal RSI;
controllo degli accessi	Ogni terminale avrà la sua password che verrà variata ogni 6 mesi, tale password non potrà essere di tipo facilmente individuabile; (le password dovranno essere consegnate in busta chiusa al custode della parola chiave)
controllo aggiornati antivirus	Verrà effettuato un controllo periodico dei sistemi adottati contro le intrusioni esterne;
controllo supporti consegnati in manutenzione	Gli archivi presenti sui supporti dati in manutenzione saranno cancellati;
rilevazione di intercettazioni	E' attivo il sistema "Fire Wall" (che riconosce i tentativi di intrusione all'interno della rete);
controllo sull'operato degli addetti alla manutenzione	Le manutenzioni HW e SW di qualsiasi genere sono effettuate dall'RSI o da esterni sotto la supervisione dell'RSI, all'uopo incaricati dal TdT.

6.3 MISURE DI SICUREZZA ADOTTATE DI TIPO ORGANIZZATIVO

Descrizione misura	Note ed indicazioni per la corretta applicazione
istruzioni interne	Le disposizioni presenti in questo piano vengono applicate per tutelare il diritto alla privacy di tutti coloro i cui dati verranno utilizzati nell'attività dell'azienda;
analisi dei rischi e Documento Programmatico sulla Sicurezza	Sulla base dell'analisi dei rischi è stato redatto il Documento Programmatico sulla Sicurezza. (DPIA). Tale documento sarà divulgato a tutte le funzioni aziendali.
piano di verifica delle misure adottate	E' stato programmato un piano di verifica sulle misure adottate. Tale piano è illustrato nel DPIA al capitolo 7.
piano di formazione degli incaricati	E' stato predisposto un piano di informazione e condivisione degli obiettivi da parte degli incaricati. Tale piano è illustrato nel DPIA al capitolo 8.
assegnazione incarichi	Sono stati assegnati e definiti dei ruoli, mediante lettere di incarico, per tutti coloro che dovranno provvedere all'applicazione del piano, in particolare: - Ai responsabili con funzione direttiva e organizzativa - Agli incaricati dei trattamenti e dei controlli interni
redazione di appositi mansionari	E' stato redatto e messo a disposizione di tutti gli incaricati un mansionario contenente le procedure in base alle quali prevenire la diffusione non autorizzata dei dati;

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

classificazione dei dati	<p>Per la sua specificità l'Isfort raccoglie e tratta dati personali nell'ambito dell'area ricerca non appartenenti a categorie particolari ma esclusivamente dati personali non sensibili, quali dati anagrafici, dati amministrativi, dati contrattuali, mentre i dati sensibili di natura medica, sono raccolti e gestiti ai fini della gestione del personale, che sono trattati e conservati presso il medico incaricato. In linea generale la raccolta e il trattamento di dati personali, nell'ambito delle attività prevalenti dell'Istituto, avviene a mezzo di una procedura informatizzata, soggetta a controllo. Detta procedura prevede la dichiarazione che i dati sono raccolti e trattati al solo fine di gestione della operatività aziendale, con contestuale rilascio, direttamente o anche attraverso il sito Internet, di idonea informativa di legge sul trattamento dei dati effettuato e conseguente raccolta del consenso degli stessi interessati.</p> <p>La sola eccezione riguarda i dati raccolti per le attività di formazione regolata in ambito ANSF, relativamente ai corsi per Operatori qualificati addetti alle mansioni per le attività di sicurezza previste nel trasporto ferroviario. Per la specificità dei dati raccolti nell'ambito delle predette attività di formazione regolata, l'Istituto, in applicazione del disposto della sezione 3 e degli artt. 27 e 35 del Regolamento UE 2016/679 – GDPR, ha ritenuto di effettuare la valutazione dell'impatto del trattamento previsti sulla protezione dei dati personali (DPIA), e contestualmente tutti gli adempimenti connessi, rappresentati attraverso il presente documento.</p> <p>In particolare la contestuale mappatura dei trattamenti effettuati dal Titolare, la valutazione del rischio privacy, la conduzione della DPIA per i soli trattamenti individuati come potenzialmente rischiosi, la definizione dei trattamenti individuati da notificare al garante della Privacy, la predisposizione del Registro dei rischi Privacy, la nomina del Responsabile della Protezione dei Dati (RPD/DPO).</p>
distruzione controllata dei supporti	I supporti magnetici, cartacei o di altro genere, verranno riutilizzati solo se i dati memorizzati in precedenza potranno essere eliminati in maniera sicura, altrimenti verranno distrutti.
prescrizione linee guida di sicurezza	Gli incaricati al trattamento verranno edotti sulle misure applicate per prevenire la diffusione illecita dei dati (misure redatte nel presente documento).
documentazione dei controlli periodici	Con cadenza annuale verrà effettuato un controllo sull'efficacia delle misure adottate.

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

**verifiche periodiche su dati
non corretti o non consentiti**

Verrà effettuato un check-up periodico approfondito all'interno degli archivi per verificare la presenza di dati non corretti.

7. Piano di verifica delle Misure Adottate e Registro dei trattamenti

La bontà delle misure adottate deve essere periodicamente verificata.

Durante queste operazioni di verifica, da effettuarsi al più **ogni sei mesi**, sarà data particolare importanza a :

- Verificare la bontà delle misure di anti-intrusione adottate.
- Corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati. Prevedere la disattivazione dei codici di accesso non utilizzati per più di sei mesi.
- Aggiornamento dei dispositivi antivirus
- Aggiornamento dei programmi software che trattano i dati personali.
- Integrità dei dati e delle loro copie di backup.
- Bontà di conservazione dei documenti cartacei
- Accertamento della distruzione dei supporti magnetici che non possono più essere riutilizzati
- Accertamento del livello di formazione degli incaricati. Prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta in azienda.

Di queste verifiche sarà redatto un verbale che sarà conservato, a cura del RDT, allegato al documento programmatico sulla sicurezza.

REGISTRO DEI TRATTAMENTI

Si riportano di seguito i 2 prospetti di compilazione del Registro dei Trattamenti predisposti a norma dell'art. 30, commi 1 e 2 del Regolamento Europeo, aggiornati al 15 ottobre 2021.

ISFORT S.P.A. <i>Istituto Superiore di Formazione e Ricerca per i Trasporti</i>				ALLEGATO N. ... DPIA 20.02.2020					
REGISTRO ATTIVITA' DI TRATTAMENTO (art.30, c.1, GDPR) - Area di trattamento: Direzione Formazione Attività Sicurezza Ferroviaria									
Indirizzo		MARCO ROMANI - VIA NIZZA 45 00198 ROMA		PIER LUIGI AYMERICH					
N. Telefono		06 852651		N. Telefono 3401501866					
Mail		mromani@isfort.it		Mail aymerich@isfort.it					
PEC				PEC aymerich@pec-legal.it					
Indirizzo		CESARE BORGIA - VIA NIZZA 45 00198 ROMA		Data Creazione la data di emiss GDPR					
N. Telefono		06 852651		Ultimo Aggiornamento 15.10.2021					
Mail		formazione@isfort.it		N. Schede Compilate 16 (sono le attività descritte)					
PEC				Prossima Revisione a 6 mesi dall'emissione GDPR					
no.	Descrizione	Finalità	Contitolare (eventuale rappresentante)	DATI PERSONALI			SICUREZZA		
				Categoria	Dati Particolari SI/NO	Termine Ultimo Cancellazione	Categoria	Consenso (SI/NO)	Misure Tecniche ed organizzative adottate (e rimandi ad eventuali allegati di dettaglio)
1	raccolta schede iscrizione	adesione al corso	AdT/CdF/NIPS	dati personali	NO	nota 1	partec con req	SI	si veda DPIA
2	individuazione candidati	definiz numero partecipanti	AdT/CdF/NIPS - RdT	dati personali	NO	nota 1	partec con req	SI	si veda DPIA
3	selezione candidati	verifica requisiti/certificazioni	AdT/CdF/NIPS - RdT	idoneità fisica	SI	nota 1	partec con req	SI	si veda DPIA
4	somministrazione test d'ingresso	verifica requisiti/certificazioni	RdT/CdF	idoneità attit	SI	nota 1	partec con req	SI	si veda DPIA
5	colloqui individuali con candidati	verifica livello di competenza	RdT/CdF	idon compet	SI	nota 1	partec con req	SI	si veda DPIA
6	definizione graduatoria	creazione elenco partecip	RdT/CdF	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
7	gestione fase inserimento candid	sottoscriz contratto corso	AdT/CdF/NIPS - RdT - AdT/CdF/RQ	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
8	gestione pratiche individuali	creazione anagrafiche	AdT/CdF/NIPS	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
9	comunicazione iscritti	ammissione al corso	AdT/CdF/NIPS - RdT	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
10	trasferimento dati su Dropbox	creazione files operativi corso	AdT/CdF/NIPS	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
11	trasferimento dati condivisi	abilitaz accessi files Dropbox	AdT/CdF/NIPS	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
12	gestione files Dropbox	trattamento/ consultazione	AdT/CdF/NIPS + autorizzati	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
13	attività di aula	erogazione corsi	AdT/CdF/NIPS - RdT	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
14	rilascio certific avvenuta formaz	ammissione esami ANSF	AdT/CdF/NIPS - RdT - AdT/CdF/RQ	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
15	verifica possesso Green Pass	per ammissione agli uffici	AdT/ AdT/VGP	dati sensibili	SI	nota 2	dipend e terzi	DL 127/2021	si veda DPIA
16	gestione servizi informatici	assist tecnica/gestione pwd	RSI	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA
17	supervisione processi GDPR	controllo regolarità trattamenti	RdT/CdF - TdT - DPO	dati sensibili	SI	nota 1	partec con req	SI	si veda DPIA

LEGENDA			
Tit	TITOLARE TRATTAMENTO	IndT	RESPONSABE TRATT CDF
AdT/CdF/NIPS	ADDETTO TRATT CDF	RSI	RESPONSABE SERVIZI INFORMATICI
RdT/CdF/NIPS	ADDETTO TRATT CDF/RSI	AdT/CdF/NO	ADDETTO TRATT QUALITA' CDF

NOTA 1 I dati sono cancellati a scadenza iscrizione/gestione pratiche/ a richiesta cancellazione dell'interessato
NOTA 2 L'App di verifica non consente ritev e conserv dati pers

ISFORT S.P.A.
 Istituto Superiore di Formazione e Ricerca per i Trasporti
 Via Nizza, 45 00198 ROMA

REGISTRO CATEGORIE DI ATTIVITA' DI TRATTAMENTO (art.30, c.2, GDPR)			
TITOLARE DEL TRATTAMENTO TdT		RESPONSABILE DEL TRATTAMENTO Rdt/ CdF	
Indirizzo	MARCO ROMANI - VIA NIZZA 45 00198 ROMA	Indirizzo	CESARE BORGIA - VIA NIZZA 45 00198 ROMA
N. Telefono	06 852651	N. Telefono	06 852651
Mail	mromani@isfort.it	Mail	formazione@isfort.it
PEC		PEC	
DELEGATO/RAPPRESENTANTE DAL TITOLARE (eventuale)		DATA PROTECTION OFFICER	
Indirizzo		Indirizzo	PIER LUIGI AYMERICI
N. Telefono		N. Telefono	340 1501866
Mail		Mail	aymerici@sbsconsultinggroup.eu
PEC		PEC	aymerici@pec-legal.it
		Registro Tenuto Da	Adt/ CdF/ NIPS
		Data Creazione	la data di emiss GDPR
		Ultimo Aggiornamento	15.10.2021
		N. Schede Compilate	15 (sono le attività descritte)
		Prossima Revisione	a 6 mesi dall'emissione GDPR

n. ordine	Descrizione	TRATTAMENTO		TRASFERIMENTI	SICUREZZA
		Finalità	Contitolare	Paesei terzi, org.ni	Misure Tecniche ed
1	dati personali candidato al corso	ammissione	RdT/ CdF	NA	cfr DPIA
2	verifica possesso GP	DL 127/2021	AdT/ RdT	NA	cfr DPIA

8. Piano di Informazione e condivisione degli obiettivi

Il presente DPIA è lo strumento essenziale per l'applicazione all'interno di Isfort del nuovo approccio alla protezione dei dati personali, Regolamento UE 2016/679 – GDPR, voluto in sede comunitaria, e fortemente incentrato sul principio della responsabilizzazione e condivisione dei principi e delle procedure di protezione dei dati personali (cd. **accountability principle**). In ragione di ciò saranno portate a conoscenza di tutti gli incaricati, in primis e del resto della struttura, le informazioni e i nuovi principi che regolano le politiche di **accountability** approvate da Isfort e contestualmente gli incaricati saranno edotti sui “rischi individuati e sui modi per prevenire i danni”

Idonea informativa (allegato n. 4), che affronterà i seguenti punti, sarà messa a disposizione di tutte le risorse aziendali, e sarà inclusa nelle lettere di incarico agli addetti al trattamento:

- Una analisi e aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee
- Disposizioni legislative in tema di tutela dei dati e criminalità informatica
- Analisi delle norme in materia di protezione dei dati personali con particolare riferimento al Regolamento UE 2016/679 – GDPR
- Analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato
- Panoramica sugli adempimenti ex Regolamento UE 2016/679 – GDPR: notificazione, rapporti con gli interessati, rapporti con il Garante.
- L'Ufficio del Garante della Privacy.
- Misure minime ed appropriate di sicurezza con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus e misure antihacker), contenitori di sicurezza, sistemi anti-intrusione, importanza e modalità di realizzazione delle operazioni di backup, etc..

Detta informativa sarà illustrata, inoltre, nel corso di una iniziativa di responsabilizzazione e condivisione dei principi e delle procedure di protezione dei dati personali all'uopo organizzata per tutta struttura, unitamente alle rispettive comunicazioni agli addetti, relative al rispetto, nell'ambito delle funzioni, compiti e mansioni attribuiti dall'Istituto, della normativa vigente e dei regolamenti interni in materia di tutela dei dati personali (allegati n. 5, n. 6, n.7, n. 8, n. 9, n. 10).

Agli addetti al trattamento, con specifiche comunicazioni di incarico, da parte del Titolare del Trattamento, saranno date **precise istruzioni su funzioni e compiti**, con riferimento sia alle norme che alle disposizioni interne del Manuale della Qualità, richiedendo la più scrupolosa osservanza delle informazioni e delle disposizioni impartite in relazione alle funzioni delegate. Le istruzioni agli addetti preciseranno le modalità di raccolta e trattamento dati personali senza l'uso di strumenti elettronici, ovvero raccolta e trattamento dati personali in modalità cartacea, fotocopiatura/ scansione con la finalità di trattamento autorizzato e modalità di raccolta e trattamento se si utilizza uno strumento elettronico (pc

ISFORT S.P.A.

Istituto Superiore di Formazione e Ricerca per i Trasporti
Via Nizza, 45 00198 ROMA

fisso, mobile, cellulare, supporti rimovibili) con sistema di autenticazione informatica e credenziali d'autenticazione abilitate dal Responsabile Sistema Informativo, su delega del Titolare del Trattamento.

Coerentemente con lo sviluppo delle attività di Isfort che comportino trattamento di dati personali, con l'evoluzione degli strumenti tecnici adottati dall'Istituto e/o con l'insorgere di nuove disposizioni legislative in materia, si provvederà ad aggiornare detta informativa.

In seguito, dopo 12 mesi dall'avvio della nuova procedura come da DPIA, qualora se ne evidenzi la necessità, si potrà organizzare un incontro per sensibilizzare gli incaricati sull'importanza di più idoneamente conformarsi alle norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

9. Appendice: Soglie di Rischio

Soglia	Descrizione
Lieve	Con questa soglia viene individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
Media	Con questa soglia viene individuato un rischio superiore al precedente identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
Grave o Gravissimo	Trattate insieme, perché con queste soglie vengono individuati rischi che è sicuramente inaccettabile pensare di correre. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio e contenerlo in livelli accettabili.

ALLEGATI

ELENCO DEGLI ALLEGATI

1. Organigramma della Società
2. Pianta dei locali aziendali
3. Architettura rete informatica interna
4. Informativa alle risorse aziendali
5. Incarico e istruzioni RdT/CdF
6. Incarico e istruzioni RSI
7. Incarico e istruzioni AdT/IS
8. Incarico e istruzioni AdT/CdF/NIPS
9. Incarico e istruzioni AdT/CdF/NIPi
10. Incarico e istruzioni AdT/CdF/RQ
11. Nomina RPD/DPO
12. Registro dei Trattamenti (art. 30, comma 1, Regolamento Europeo 679/2016)
13. Registro dei Trattamenti (art. 30, comma 2, Regolamento Europeo 679/2016)
14. Protocollo per la verifica del possesso della Certificazione Verde per l'accesso nei luoghi di lavoro dell'Azienda, 15 ottobre 2021, di applicazione del D.L. n. 127/2021
15. Registro Verifica del possesso della Certificazione Verde
16. Incarico e istruzioni Addetto Verifica Green Pass AdT/ CGP

Data, 15 ottobre 2021

Il Titolare del trattamento