DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Valutazione di Impatto sulla Protezione dei Dati Personali ex art. 35 Reg. EU 2016/679 (c.d. "GDPR") (*Data Protection Impact Assessment*)

Oggetto	**DPIA Piattaforma "FACILITA"**
Stato del progetto	**Pre-rilascio***
Documento redatto da	**Dipartimento per la Trasformazione Digitale in collaborazione con responsabili del trattamento**
Data di ultimo aggiornamento	**8/3/2024**
Versione	**v.1 Consolidata***

INDICE

1. Descrizione sistematica del trattamento (articolo 35, paragrafo 7, lettera a)

1.1. La natura, l'ambito di applicazione, il contesto e le finalità del trattamento (considerando 90)

La misura 1.7.2 del PNRR

All'interno del Piano Nazionale di Ripresa e Resilienza sono previsti diversi interventi con l'obiettivo di garantire ai cittadini italiani opportunità di alfabetizzazione digitale e formazione su tematiche afferenti ai servizi digitali della Pubblica Amministrazione.

In particolare, la Missione 1 - Componente 1 - Asse 1 - Misura 1.7.2 "Rete di servizi di facilitazione digitale" è dedicata all'attivazione o potenziamento dei "Centri di facilitazione digitale": punti di accesso fisici che forniscono ai cittadini formazione sia online che di persona con l'obiettivo di ottenere competenze digitali e supportare l'inclusione digitale.

Il soggetto titolare della misura 1.7.2 (definizione da non confondere, in questa DPIA, con la definizione di Titolare del Trattamento) è il **Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri** (di seguito indicato "DTD").

I soggetti attuatori della misura 1.7.2 sono individuati nelle **Regioni** e nelle **Province autonome** che hanno redatto un Piano Operativo.

I soggetti sub-attuatori della misura 1.7.2 possono essere In-House, Comuni, Enti del Terzo Settore, sulla base del Piano Operativo (possono essere anche le Regioni o Province autonome stesse).

I soggetti che erogano le attività di facilitazione digitale ai cittadini, nell'ambito della misura 1.7.2., sono i **Facilitatori** digitali che possono essere dipendenti pubblici, del terzo settore o assunti *ad hoc*, ed operano presso le sedi dei sub-attuatori o delle Regioni o Province autonome.

Tra il DTD e i soggetto attuatori è stato stipulato apposito accordo ai sensi dell'articolo 15, legge 7 agosto 1990, n. 241 per la realizzazione della misura 1.7.2 "Rete dei servizi di facilitazione digitale" (di seguito indicato "accordo principale") nonchè un accordo integrativo (di seguito indicato "accordo integrativo") contenente una definizione puntuale circa i ruoli, attività e le relative basi giuridiche attinenti al trattamento dei dati personali in specifica all'articolo 5, paragrafo 2, lettera B dell'accordo principale. Tale accordo integrativo è stato oggetto di specifica approvazione da parte della Commissione Affari istituzionali e generali della Conferenza delle Regioni e delle Province autonome nella seduta del 19/12/2023.

In particolare, l'accordo integrativo individua le seguenti **attività** nell'ambito del trattamento dati relativo all'intervento di cui alla Misura 1.7.2 PNRR e, nello specifico:

1. **monitoraggio e verifica della Misura 1.7.2 e del collegato target M1C1-28**. Nello specifico, il target in questione (M1C1- 28) espresso come "*At least two million citizens participating in training initiatives provided by digital facilitation centres*" prevede il raggiungimento (e il conseguente conteggio) di almeno 2 milioni di cittadini che hanno partecipato a iniziative di facilitazione digitale.
2. **messa a disposizione di un sistema informativo di gestione della conoscenza tra i Facilitatori** che favorisce la condivisione di best practice da parte degli enti coinvolti, la comunicazione tra i soggetti coinvolti ed il facile accesso a materiale utile per l'erogazione dei servizi da parte dei facilitatori.
3. **erogazione di attività di formazione** per gli operatori che assumono il ruolo di facilitatori.

L'accordo integrativo stipulato prevede altresì che il DTD metta a disposizione dei soggetti attuatori, la Valutazione di impatto privacy sulla protezione dei dati personali effettuata ai sensi dell'articolo 35 del GDPR realizzata per quanto di propria competenza.

1.2. Descrizione funzionale del trattamento

Funzionamento della piattaforma "Facilita"

A supporto di queste iniziative, il DTD ha progettato "Facilita", una **piattaforma** che consente sia il monitoraggio e la verifica delle attività di facilitazione digitale svolte sul territorio, necessari ai sensi del PNRR, sia la messa a disposizione, in particolare ai facilitatori, di un sistema di *knowledge management.* Quest'ultimo favorisce la condivisione di buone pratiche da parte degli enti coinvolti e comunicazione ed accesso a materiale utile per l'erogazione delle attività di facilitazione da parte dei Facilitatori.

Ad esclusione dei cittadini, "Facilita" consente la creazione di diversi profili **utente**.

Ad ogni utente sono assegnati dei profili specifici (*set* di permessi) che consentono di differenziare la messa a disposizione di funzionalità tecniche e il trattamento di dati all'interno della piattaforma.

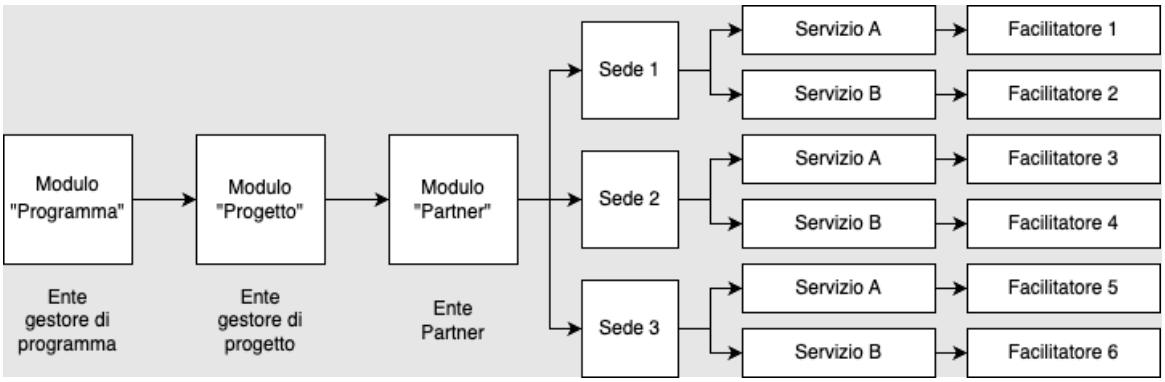
L'accesso alla piattaforma da parte degli utenti avviene con SPID o CIE, livello di sicurezza LoA2. Al primo accesso, ogni utente autenticato completa la registrazione dei campi obbligatori e prende visione dell'informativa privacy. Ad ogni utente viene associato un ID.

Nel proseguo della navigazione, l'utente ha accesso ad un menù di navigazione: in base ruolo assegnato ed al relativo set di permessi concessi potrà avere accesso a diverse funzionalità.

Nello specifico, a livello informatico, in piattaforma sono identificate entità **Programma** ed entità **Progetto** (queste ultime facenti riferimento alle prime) ciascuna delle quali ha come riferimento rispettivamente un **Ente Gestore di Programma** o un **Ente Gestore di Progetto**. Per il Progetto poi viene identificato un'entità **Partner**, all'interno della quale, suddivisi per tutte le **sedi** afferenti a quell'Ente, sono registrati gli **utenti**.

Gli utenti (i Facilitatori digitali) vengono identificati, a livello informatico, con il solo profilo di **Facilitatori** e, come detto, sono coloro che si occupano di attuare le attività di facilitazione digitale. Ogni attività è identificata su Facilita come **Servizio**.

Nella seguente figura è rappresentato il flusso identificativo dei profili.



Una volta terminata l'attività di facilitazione nei confronti dei cittadini, viene generato un **questionario di rilevazione dell'esperienza**, che il Facilitatore pone al cittadino che ne ha fruito, formulando le domande in presenza o consegnando all'interessato una copia del questionario stampata affinché la compili insieme al Facilitatore.

Conteggio delle attività di facilitazione erogate e pseudonimizzazione

Le risposte al questionario di rilevazione dell'esperienza devono essere inserite su "Facilita" ed associate al cittadino. A tale proposito, al fine di mettere a disposizione una misura di sicurezza che consenta di non identificare direttamente i cittadini, all'atto dell'inserimento del Codice Fiscale (del cittadino) quest'ultimo, dopo essere stato verificato e validato, viene pseudonimizzato nell'ambiente locale del Facilitatore unitamente ad altri dati che sono rilevati al momento, come Genere, Fascia d'età, Stato Occupazionale, Titolo di Studio (livello più alto raggiunto), Provincia di Domicilio, Cittadinanza insieme alle attività di facilitazione per le quali il cittadino ha richiesto il servizio.

La soluzione di crittografia dei dati utilizzata si basa sull'algoritmo AES (Advanced Encryption Standard), una tecnica di crittografia a chiave simmetrica sicura e affidabile per proteggere i dati. AES utilizza la stessa chiave per crittografare e decrittografare i dati, semplificando il processo senza compromettere la sicurezza; per garantire la privacy e l'anonimizzazione dei dati dei cittadini, come ad esempio il codice fiscale, è stata implementata una procedura aggiuntiva che consente di convertire il codice fiscale in un array di byte utilizzando l'encoding UTF-8.

Una volta convertito il CF, l'algoritmo di hash SHA-256, noto anche per la sua robustezza e resistenza, genera un codice univoco fornito dal processore in modo da fornire una rappresentazione, univoca e non reversibile, dei dati originali.

Per ottenere una rappresentazione più leggibile e gestibile dell'hash, ogni byte viene convertito in una stringa esadecimale così da ottenere una rappresentazione del dato in un formato più compatto e facilmente memorizzabile nel database.

Il processo di crittografia AES utilizzato in Facilita, in combinazione con la tecnica di hashing, garantisce l'irreversibilità dei dati crittografati. Quindi, in Facilita tali dati sono abbinati ad un codice alfanumerico derivato da una codifica irreversibile del codice fiscale, che rende impossibile associarli ad un cittadino identificato (in assenza del codice fiscale poi cifrato) ma nello stesso tempo consente di contare univocamente il cittadino che ha usufruito dei servizi di facilitazione come richiesto dal target PNRR sopra citato, al solo scopo di utilizzare tali dati per finalità di monitoraggio e verifica PNRR dei servizi svolti*.

In figura lo schema dei dati del questionario di rilevazione dell'esperienza dati che il Facilitatore carica in Facilita*.

REGIONE O PROVINCIA AUTONOMA			**SEDE di svolgimento attività** (Città, Provincia, indirizzo, CAP.....)	
CUP (Codice Unico Progetto)			**OPERATORE VOLONTARIO** (Nome e Cognome)	
ENTE TITOLARE del Programma di Intervento			**DATA**	aaaa-mm-gg
TITOLO del Progetto			**DURATA DELL'ATTIVITA'**	hh:mm
DATI ANAGRAFICI CITTADINO			**TIPOLOGIA DI ATTIVITA' SVOLTA*** (indicare una delle voci presenti nelle celle sottostanti)	
CODICE IDENTIFICATIVO UNICO			***FACILITAZIONE DIGITALE*** *(supporto all'accesso a servizi pubblici o altri servizi) **	***Formato Apprendimento*** *(Frontale/Non Frontale)*
GENERE			Servizi Pubblici	
FASCIA DI ETA'			***EDUCAZIONE DIGITALE*** *(nell'ambito delle 5 aree DigComp) ****	***Formato Apprendimento*** *(Frontale/Non Frontale)*
CITTADINANZA			Alfabetizzazione	
PROVINCIA DI RESIDENZA			Comunicazione	
TITOLO DI STUDIO			Creazione Contenuti	
OCCUPAZIONE			Sicurezza	
			Soluzione Problemi	
Numero e data dell'attività				

NOTA DI DETTAGLIO SULLA TIPOLOGIA DI ATTIVITA': "Facilitazione digitale**" fanno parte di questa tipologia i servizi che offrono supporto individuale all'utenza di servizi online (attraverso, per esempio, punti di assistenza digitale già operanti nell'Ente, anche itineranti), oppure i servizi che si intende realizzare ex novo come sostegno delle proprie attività di assistenza all'utenza. Tale attività si concretizza in momenti di supporto e affiancamento individualizzati, che mirano ad incidere sulla motivazione e l'auto-efficacia, sull'approccio al digitale, e sul co*
*" **Educazione digitale**" rientrano in questa tipologia i servizi, che riguardano l'educazione all'uso di strumenti digitali, non riferiti a servizi erogati direttamente dall'ente, con l'intento di curare la diffusione della "cultura digitale".*
***/ **Servizi Pubblici** erogati e che verranno indicati nell'Attestato includono: AppIO, PagoPA, ANPR, FSE, Servizi relativi all'istruzione, Formazione, Servizi per l'occupazione, Servizi previdenziali e assistenziali, Adempimenti Fiscali*

****Le **Competenze delle 5 Aree DigComp** che verranno indicate nell'attestato includono: Navigare e cercare dati e info, Valutare dati info e contenuti, Gestire dati info e contenuti (area Alfabetizzazione); Interagire attraverso le tecnologie, Condividere info, Esercitare la cittadinanza, Collaborare con le tecnologie digitali, Comportamento e rispetto online, Gestire l'identità digitale (area Comunicazione); Creazione di contenuti digitali (area Contenuti); Proteggere i dispositivi, Proteggere i dati personali e la privacy (area Sicurezza); Risolvere i problemi tecnici hardware*

1.3. Dati personali, destinatari e periodo di conservazione dei dati personali

Famiglia di dati	Tipo di dati	Categorie di interessati	Periodo di conservazione
Dati comuni	Nome, cognome, mail, Codice Fiscale, Numero telefono (facoltativo)	**Rappresentanti legali e referenti dei Soggetti attuatori**	Fino al termine delle verifiche UE della misura – scadenza per raggiungimento target giugno 2026.

Dati comuni	Nome, cognome, mail, Codice Fiscale, Numero telefono (facoltativo)	**Rappresentanti legali e referenti dei Soggetti Sub-attuatori**	Fino al termine delle verifiche UE della misura – scadenza per raggiungimento target giugno 2026.
Dati comuni	Nome, cognome, mail, Codice Fiscale, Numero telefono (facoltativo) associati alle attività di svolte.	**Facilitatori**	Fino al termine delle verifiche UE della misura – scadenza per raggiungimento target giugno 2026.
Dati Comuni	Dati relativi alla fruizione dei servizi di facilitazione digitale (fascia di età, genere, provincia di domicilio, etc.) dell'interessato identificato tramite codice fiscale pseudonimizzato in locale dal facilitatore tramite un sistema di codifica univoco stabilito a livello nazionale dal DTD*	**Cittadini che fruiscono dei servizi di facilitazione**	Fino al termine delle verifiche UE della misura – scadenza per raggiungimento target giugno 2026.
Log relativi alle attività degli utenti in Facilita	Dati derivanti dalle attività degli utenti che hanno accesso a Facilita quali data e ora dell'accesso/uscita, operazione richiesta; per i log applicativi dei microservizi: dati tecnici ed errori applicativi (in caso di crash); per i log dei web server; pagina richiesta; da che IP, ecc.; per i Log a livello rete della VPN: utenza che si connette/disconnette; errori di configurazione. Per ciascuna operazione effettuata è associato il relativo ID di sessione del sistema di autenticazione scelto.	**Rappresentanti legali e referenti dei soggetti Attuatori e Sub-attuatori e Facilitatori**	1 anno fatte salve esigenze di conservazione ulteriore in caso di eventuali contenziosi.
Log di sicurezza	Dati derivanti dalle attività degli Amministratori di sistema	**Amministratori di sistema**	6 mesi come da normativa fatte salve esigenze di conservazione ulteriore in caso di eventuali contenziosi.

Il trattamento dei dati personali avverrà interamente presso il DTD che mette a disposizione le proprie infrastrutture esistenti avvalendosi di **responsabili del trattamento,** opportunamente contrattualizzati. In particolare, i principali responsabili del trattamento per Facilita sono **Enterprise Services Italia S.r.l**. e **DS Tech S.r.l**., fornitori dei servizi di sviluppo, erogazione e gestione operativa della piattaforma e **Amazon Web Service EMEA SARL** (di seguito indicata "AWS").

1.4. Risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali)

Dal punto di vista tecnico di funzionamento di Facilita, per quanto qui interessa, l'infrastruttura che ospita i dati è sottoposta alle specifiche di cui all'articolo 33-septies, comma 4, del D.L. 179/2012 e all'articolo 17, comma 6, del D.L. 82/2021 e del relativo "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione" adottato da AGID con determinazione 628/2021 e relativi atti dell'Agenzia nazionale per la cybersicurezza. In particolare sono utilizzati servizi qualificati ACN - Livello di Qualificazione minimo. I dati trattati sono classificati quali dati "ordinari" ai sensi del regolamento citato.

I soggetti che possono accedere su Facilita sono identificati tramite identitià digitale, livello LoA2 e, a ciascun ruolo sono assegnati dei profili specifici (set di permessi) che consentono di determinare delle differenze nella messa a disposizione e utilizzo di determinate funzionalità e nella visualizzazione di informazioni all'interno della piattaforma.

Dettaglio dei soggetti e dei ruoli su Facilita

Amministrazione Titolare

L'amministrazione titolare della misura 1.7.2 è il DTD.

All'interno di Facilita il personale autorizzato del DTD ad operare in piattaforma opera con i profili di:

- "DTD Amministratore Misura 1.7.2" con le seguenti funzionalità e permessi:
- Si autentica tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Crea programmi di intervento della Rete di facilitazione digitale
- Associa l'ente gestore di programma e i relativi referenti/delegati
- Può agire sul programma, in termini di redazione, fino alla sede di riferimento
- Visualizza le informazioni di tutti gli utenti censiti in piattaforma e può modificarle
- Può associare nuovi ruoli a specifici utenti

- Crea nuovi ruoli 'custom', di cui può modificare i permessi ed eliminarli se necessario
- Può visualizzare, gestire e modificare i template dei questionari
- Monitora tutti i KPI relativi alle attività di facilitazione che si svolgono in piattaforma
- Accede al tool di Business Intelligence
- Crea e modifica news, topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Modera news, topic e documenti
- Modera i commenti alle news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Invia e visualizza le segnalazioni
- Gestisce le categorie

- "Moderatore" con le seguenti funzionalità e permessi:
- Si autentica tramite SPID o CIE
- Compila il suo profilo al primo accesso
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Modera news, topic e documenti
- Modera i commenti alle news, topic e documenti
- Invia e visualizza le segnalazioni
- Gestisce le categorie

Soggetti Attuatori

I soggetti attuatori della misura 1.7.2 coincidono con il profilo "Ente Gestore di Programma" che operano con i profili di:

- "Referente Ente gestore di programma" con le seguenti funzionalità e permessi:
- Si autentica tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Nomina il delegato ente gestore di programma
- Modifica e/o completa le informazioni dell'ente gestore di programma
- Modifica e/o completa le informazioni generali del programma
- Visualizza il questionario di default per il programma per cui sta operando
- Crea i progetti
- Associa l'ente gestore di progetto e i relativi referenti/delegati

- Può visualizzare le informazioni dei progetti fino alla foglia della sede
- Termina il programma
- Visualizza le informazioni degli utenti ed enti censiti operanti sui programmi per cui sta operando
- Monitora i KPI relativi alle attività di facilitazione in base all'intervento del programma per cui sta operando (SCD o RFD)
- Crea e modifica news, topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

- "Delegato Ente gestore di programma" con le seguenti funzionalità e permessi:
- Si autentica tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Modifica e/o completa le informazioni dell'ente gestore di programma
- Modifica e/o completa le informazioni generali del programma
- Visualizza il questionario di default per il programma per cui sta operando
- Crea i progetti
- Associa l'ente gestore di progetto e i relativi referenti/delegati
- Può visualizzare le informazioni dei progetti fino alla foglia della sede
- Termina il programma
- Visualizza le informazioni degli utenti ed enti censiti operanti sui programmi per cui sta operando
- Monitora i KPI relativi alle attività di facilitazione in base all'intervento del programma per cui sta operando (SCD o RFD)
- Crea e modifica news, topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

Soggetti Sub-attuatori

I Soggetti Sub-attuatori della misura 1.7.2 coincidono con il profilo "Ente Gestore di Progetto" oppure "Ente Partner "e operano con i profili di:

- "Referente Ente gestore di progetto" con le seguenti funzionalità e permessi:

- Si autentica tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Nomina il delegato ente gestore di progetto
- Modifica e/o completa le informazioni dell'ente gestore di progetto
- Modifica e/o completa le informazioni generali del progetto
- Associa l'ente gestore partner e i relativi referenti/delegati
- Può censire sedi e aggiungere facilitatori
- Attiva il progetto
- Termina il progetto
- Visualizza le informazioni degli utenti ed enti censiti operanti sui progetti per cui sta operando
- Visualizza le informazioni dei servizi relativi al progetto di riferimento
- Monitora i KPI relativi alle attività di facilitazione in base all'intervento del programma per cui sta operando (SCD o RFD)
- Crea e modifica news, topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

- Delegato Ente gestore di progetto con le seguenti funzionalità e permessi:

- Si autentica in piattaforma tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Modifica e/o completa le informazioni dell'ente gestore di progetto
- Modifica e/o completa le informazioni generali del progetto
- Associa l'ente gestore partner e i relativi referenti/delegati
- Può censire sedi e aggiungere facilitatori
- Attiva il progetto
- Termina il progetto
- Visualizza le informazioni degli utenti ed enti censiti operanti sui progetti per cui sta operando
- Visualizza le informazioni dei servizi relativi al progetto di riferimento
- Monitora i KPI relativi alle attività di facilitazione in base all'intervento del programma per cui sta operando
- Crea e modifica news, topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti

- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

- Referente Ente partner con le seguenti funzionalità e permessi:
- Si autentica in piattaforma tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Nomina il delegato ente partner
- Censisce sedi e aggiunge facilitatori
- Visualizza le informazioni degli utenti ed enti censiti operanti sui progetti per cui sta operando
- Visualizza le informazioni dei servizi relativi al progetto di riferimento
- Monitora i KPI relativi alle attività di facilitazione in base all'intervento del programma per cui sta operando
- Crea e modifica topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

- Delegato Ente partner con le seguenti funzionalità e permessi:
- Si autentica in piattaforma tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso
- Censisce sedi e aggiunge facilitatori
- Visualizza le informazioni degli utenti ed enti censiti operanti sui progetti per cui sta operando
- Visualizza le informazioni dei servizi relativi al progetto di riferimento
- Monitora i KPI relativi alle attività di facilitazione in base all'intervento del programma per cui sta operando
- Crea e modifica topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

- "Facilitatore" con le seguenti funzionalità e permessi:
- Si autentica in piattaforma tramite SPID o CIE
- Completa i suoi dati anagrafici al primo accesso

- Crea i servizi
- Aggiunge cittadini
- Somministra i questionari ai cittadini
- Visualizza le informazioni dei cittadini partecipanti ai servizi che ha creato
- Crea e modifica topic e documenti
- Visualizza news, topic e documenti
- Commenta news, topic e documenti
- Visualizza i suoi contenuti pubblicati
- Segnala contenuti e/o commenti

In aggiunta, è previsto uno specifico profilo **"**Gestore dei facilitatori" che è un "ruolo custom" che può essere creato dal profilo "DTD Amministratore Misura 1.7.2" direttamente in Facilita. Il "Gestore dei facilitatori" disporrà di una visualizzazione non specifica ma generale. Per questo tipo di ruolo è possibile modificare i permessi. Ad esempio: se un utente con ruolo custom viene abilitato al permesso per la lettura lista progetti, il cono di visibilità consente la visualizzazione di tutti i progetti censiti in piattaforma.

I log applicativi, di sistema e di sicurezza vengono gestiti dal DTD secondo normativa.

Non sono applicabili codici di condotta (articolo 35, paragrafo 8).

2. Necessità e la proporzionalità (articolo 35, paragrafo 7, lettera b)

In questa fase si procede ad un'analisi della necessità e della proporzionalità del trattamento rispetto alle finalità, con l'intenzione di rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate dal DTD.

2.1. Misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90)

2.1.1. Misure che contribuiscono alla proporzionalità e alla necessità del trattamento

2.1.1.1. Finalità determinate, esplicite e legittime (art. 5, par. 1, lettera b)

Le finalità relative al trattamento dei dati da parte del DTD sono strettamente connesse all'intervento di cui alla Misura 1.7.2 PNRR e, nello specifico:

1) monitoraggio e verifica della Misura 1.7.2 e del collegato target M1C1-28;
2) messa a disposizione di un sistema informativo di gestione della conoscenza tra i Facilitatori;
3) Erogazione di attività di formazione per gli operatori che assumono il ruolo di facilitatori .

2.1.1.2. liceità del trattamento (art. 6)

I dati sono trattati nell'esecuzione dei compiti di interesse pubblico o comunque connessi all'esercizio dei pubblici poteri in conformità all'art. 6, paragrafo 1, lett. e) del GDPR nonché per obbligo di legge in conformità all'art. 6, paragrafo 1, lett. c) del GDPR per lo svolgimento delle attività correlate agli obblighi di monitoraggio e verifica del target europeo PNRR M1C1-28 legato alla misura 1.7.2..

In particolare, si evidenziano gli obblighi derivanti da:

- Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio, del 12 febbraio 2021, che istituisce il dispositivo per la ripresa e la resilienza e ss.mm. nonchè la normativa nazionale di riferimento e, in particolare la normativa indicata al punto successivo per quanto riguarda gli obblighi di monitoraggio e verifica;
- Articolo 5 del decreto-legge 24 febbraio 2023, n. 13 convertito, con modificazioni, dalla legge 21 aprile 2023, n. 41, rubricato "Disposizioni in materia di controllo e monitoraggio dell'attuazione degli interventi realizzati con risorse nazionali ed europee" e relativo decreto attuativo in corso di emanazione*;
- articolo 2-ter del decreto legislativo 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- Accordo principale e integrativo tra DTD e soggetti attuatori stiupulato ai sensi dell'articolo 15, legge 7 agosto 1990, n. 241 per la realizzazione della misura 1.7.2 "Rete dei servizi di facilitazione digitale" .

2.1.1.3. dati personali adeguati, pertinenti e limitati a quanto necessario (art. 5, paragrafo 1, lettera c)

I dati trattati sono quelli minimi per garantire il corretto monitoraggio della misura ed adempiere agli ulteriori obblighi a supporto della misura (ambiente di knowledge management ed erogazione della formazione per i Facilitatori).

Per quanto riguarda il monitoraggio, i dati sono stati opportunamente configurati utilizzando intervalli numerici ampi e scale o ordini di grandezza efficaci, in modo da evitare i cosiddetti "quasi identificatori" ed escludere il rischio di individuazione, correlabilità e deduzione dell'identità del cittadino (es. fascia di età, area geografica) oltre che pseudonimizzati*.

2.1.1.4. limitazione della conservazione (art. 5, paragrafo 1, lettera e)

La reportistica finalizzata al monitoraggio e verifica della misura 1.7.2 verrà generata a giugno 2026 e i dati saranno mantenuti fino al termine delle verifiche UE sulla misura.

I log sono mantenuti secondo normativa e il periodo minimo di conservazione di quelli relativi agli utenti autorizzati ad operare in Facilita è determinato in un anno, fatte salve esigenze di conservazione ulteriore in caso di eventuali contenziosi.

2.1.2. Misure che contribuiscono ai diritti degli interessati

2.1.2.1. informazioni fornite all'interessato (artt. 12, 13 e 14)

L'informativa relativa al trattamento dei dati viene fornita agli interessati secondo quanto previsto nell'accordo integrativo sopra citato.

Nello specifico:

- Il DTD mette a disposizione **dei rappresentanti o delegati dei soggetti attuatori e sub-attuatori nonchè dei facilitatori** un'informativa ai sensi degli articoli 13 e 14 del GDPR di cui viene richiesta conferma di lettura all'utente al momento della registrazione o del primo accesso in Facilita.
- Il DTD mette a disposizione dei **cittadini** un'informativa ai sensi dell'articolo 14 del GDPR in una pagina dedicata alla misura.

2.1.2.2. diritto di accesso e portabilità dei dati (artt. 15 e 20)

Il diritto di accesso "di ottenere dal titolare del trattamento la conferma che sia in corso o meno un trattamento dei dati personali che lo riguardano" può essere esercitato da parte **dei rappresentanti o delegati dei soggetti attuatori e sub-attuatori nonchè dei facilitatori** accedendo

a Facilita ovvero inviando una comunicazione ai dati di contatto del Titolare.

I **cittadini** possono esercitare il diritto di accesso previa comunicazione ai dati di contatto del Titolare del codice fiscale da cui è possibile ricavare lo pseudonimo associato*.

Il diritto alla portabilità non è esercitabile poiché non ricorrono i presupposti di cui all'art. 20 (trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento).

2.1.2.3. diritto di rettifica e alla cancellazione (artt. 16, 17 e 19)

I rappresentanti o delegati dei soggetti attuatori e sub-attuatori nonchè i facilitatori hanno diritto a rettificare dati inesatti o integrarli. I dati potranno essere verificati e rettificati dall'interessato al primo accesso in Piattaforma. Nei casi di legge, hanno diritto a chiedere l'oblio ma la cancellazione dei dati potrà avvenire solo a seguito della conclusione dell'attività di facilitazione, monitoraggio e verifica della misura.

Il **cittadino** non ha diritto a rettificare i propri dati. Come specificato, il codice fiscale del Cittadino viene immediatamente pseudonimizzato e dunque non viene trattato da Facilita*. Con riguardo alla stringa alfanumerica, seppur considerabile dato personale, necessita di essere mantenuta nella sua conformazione ai fini di monitoraggio e verifica delle misure. Nei casi di legge, il cittadino ha diritto a chiedere l'oblio ma la cancellazione dei dati (stringa alfanumerica) potrà avvenire solo a seguito della conclusione dell'attività di facilitazione, monitoraggio e verifica della misura*.

2.1.2.4. diritto di opposizione e di limitazione di trattamento (art. 18, 19 e 21)

Per particolari motivi e nei casi di legge previsti, è garantito il diritto di opporsi al trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

2.1.2.5. rapporti con i responsabili del trattamento (art. 28)

Tutti i responsabili del trattamento sono opportunamente contrattualizzati.

2.1.2.6. garanzie riguardanti trattamenti internazionali (capo V)

Per quanto attiene allo specifico servizio cloud a supporto dell'infrastruttura su cui poggia l'esecuzione di Facilita, il DTD si avvale dei servizi cloud forniti da Fastweb S.p.A. su AWS. Il servizio cloud in oggetto è qualificato ACN QC2 ed opera in ambito security adottando il concetto di "region" e "modello di responsabilità condivisa".

Per "region" si intende il luogo fisico nel mondo in cui si clusterizzano i data center e nello specifico la region dedicata a Facilita è Francoforte (Germania).

In ogni caso, si segnala che il *Cloud Service Provider* di riferimento integra le c.d. SCC, clausole contrattuali standard, adottate dalla Commissione europea (CE) nel giugno 2021. Tutti i servizi forniti da AWS, oltre che dallo specifico contratto, sono disciplinati anche dagli AWS Service Terms (amazon.com) che, all'art. 1.14, contengono il riferimento al DPA aws-dpa.pdf (awsstatic.com). Oltre al DPA, è presente anche un Supplementary Addendum al DPA (supplementary-addendum-to-the-aws-dpa.pdf (awsstatic.com) con l'indicazione di alcune misure aggiuntive adottate da AWS a tutela dei dati degli interessati.

2.1.2.7. consultazione preventiva (articolo 36)

Non è necessaria una consultazione preventiva ai sensi dell'articolo 36 GDPR.

3. Rischi per i diritti e le libertà degli interessati* (art. 35, par. 7, lett. c)

3.1. l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84)

Di seguito si analizzano:

- le fonti di rischio (considerando 90);
- gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
- le minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e l'indisponibilità dei dati (secondo più recenti studi condotti in merito alle minacce cybersecurity sia a livello italiano ed europeo ed, in particolare, 1) ENISA Threat Landscape 2023, ottobre 2023 e 2) Rapporto CLUSIT, edizione di metà anno, ottobre 2023);
- la stima della probabilità e della gravità (considerando 90).

È utilizzato un modello qualitativo di valutazione "alto", "medio", "basso" in linea con quelli proposti nelle proprie linee guida sul "privacy risk management" da ENISA (European Network and Information Security Agency) o da CNIL (Commission nationale de l'informatique et des libertés, l'Autorità francese per la protezione dei dati).

Si segnala che mentre l'impatto potenziale per i diritti e le libertà degli interessati, in relazione alla integrità e disponibilità dei dati, non crea particolari difficoltà all'interessato, quello in relazione alla riservatezza può creare minime difficoltà (ad esempio costi, mancato accesso a servizi, incomprensioni, stress, malanni minori) a causa degli effetti sulla vita lavorativa o personale degli interessati in termini di perdita di autonomia; esclusione; perdita di libertà; squilibrio di potere; perdita di fiducia; perdita economica (definibile complessivamente e considerato secondo un modello qualitativo quale, ad esempio, quello proposto nelle proprie linee guida sul "privacy risk management" da ENISA o da CNIL come "limitato" o "basso").

Nello stesso senso, la probabilità e la gravità del rischio riguardo alla integrità, disponibilità dei dati e riservatezza sono da valutarsi tenuto conto della probabilità di accadimento nell'odierno contesto internazionale, l'affinamento delle modalità di intrusione, la frequenza di incidenti nel settore pubblico, l'attrattività dei dati in uno scenario realistico in termini di appetibilità dell'obiettivo e il numero di interessati che in questo caso, per impostazione predefinita*, sono limitati (definibile complessivamente e secondo un modello qualitativo quale, ad esempio, quello proposto nelle proprie linee guida sul "privacy risk management" da ENISA o da CNIL come "medio").

Il rischio iniziale di partenza, pertanto, è complessivamente classificato quale rischio "medio".

Nelle tabelle che seguono si riporta il dettaglio delle valutazioni effettuate sul rischio iniziale.

*Legenda: **P**: Probabilità. **I:** Impatto. **RI:** Rischio Iniziale*

Perdita di riservatezza	**P**	**I**	**RI**	**Motivazione**
Attacco Hacker	**Medio**	**Basso**	**Medio**	Gli attacchi cyber proliferano in maniera esponenziale poiché sono cresciuti sia il numero sia la tipologia di software malevoli, che appaiono sempre più sofisticati. "Facilita" è un applicativo web, quindi esposto a potenziali attacchi (es. Sql Injection, attacco DDOS, Malware web based, Bad bot) tali da impattare sulla riservatezza dei dati. Tuttavia, l'appetibilità dei dati è limitata e l'impatto potenziale per gli interessati può creare minime difficoltà.
Diffusione di malware	**Alto**	**Basso**	**Medio**	Il malware può infiltrarsi sui sistemi informatici e le reti attraverso vari mezzi, sfruttando spesso le vulnerabilità nei software, debolezze nei protocolli di sicurezza o comportamento umano ignaro. L'attacco prescinde dall'appetibilità dei dati. L'impatto potenziale per gli interessati può creare minime difficoltà.
Divulgazioni di Informazioni	**Medio**	**Basso**	**Medio**	La probabilità è media in quanto le divulgazioni delle informazioni possono avvenire anche inconsapevolmente.
Errore umano	**Medio**	**Basso**	**Medio**	Il fattore umano è l'anello più debole della sicurezza e rende spesso insicura un'infrastruttura tecnologica.
Furto di identità	**Alto**	**Basso**	**Medio**	Minaccia reale che può concretizzarsi in vari modi, grazie a tecniche sempre più sofisticate utilizzando sistemi come per esempio il phishing e malware per rubare le informazioni private degli individui.
Malfunzionamento del software	**Alto**	**Basso**	**Medio**	I difetti di un prodotto software sono sempre presenti in una certa misura e ciò non dipende da una disattenzione o irresponsabilità dello sviluppatore, ma perché la complessità del software è generalmente

				intrattabile e gli uomini hanno capacità limitate per gestire la complessità. Una prima tipologia di difetti che si possono presentare in un'applicazione sono quelli rilevabili da malfunzionamenti del software in fase di esecuzione, solitamente causati da difetti di design applicativo o da difetti di codice.
Manomissione Software	**Alto**	**Basso**	**Medio**	La manomissione dei software può causare gravi incidenti di sicurezza. In "Facilita", gli autori malintenzionati possono spacciare per legittime le librerie non autorizzate sfruttando "difetti logici" nei gestori di pacchetti open source. Ad esempio, i pacchetti contenenti malware possono essere attribuiti a manutentori fidati a loro insaputa. Tale fiducia mal riposta può introdurre vulnerabilità problematiche e nascoste nel codice. Queste vulnerabilità possono fornire agli aggressori l'accesso a dati e consentire loro di installare malware e sistemi di controllo lungo tutta la catena di fornitura del software.
Phishing	**Alto**	**Basso**	**Medio**	È una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli. Se gli utenti non sono consapevoli e non hanno ricevuto la giusta formazione, possono, anche inconsapevolmente con il loro comportamento causare un notevole danno.
Uso non autorizzato di dispositivi	**Medio**	**Basso**	**Medio**	La mancata gestione degli accessi fisici e logici a dispositivi può compromettere la sicurezza del patrimonio informativo.
Abuso di privilegi	**Medio**	**Basso**	**Medio**	L'abuso di privilegi comporta diversi rischi, tra cui la compromissione di account e dati, perdite finanziarie ingenti e danni alla reputazione
Accesso non autorizzato ai dati	**Medio**	**Basso**	**Medio**	Un mancato controllo sulla gestione degli accessi logici e fisici determina un impatto in termini di riservatezza delle informazioni
Rischio generale	**Medio**	**Basso**	**Medio**	

per gli eventi di perdita di riservatezza				

Perdita di disponibilità	**P**	**I**	**RI**	**Motivazione**
Abuso dei privilegi	**Alto**	**Basso**	**Medio**	L'abuso di privilegi comporta diversi rischi, tra cui la compromissione di account e dati, perdite finanziarie e danni alla reputazione
Attacco hacker	**Medio**	**Basso**	**Medio**	Gli attacchi cyber attacchi proliferano in maniera esponenziale poiché sono cresciuti sia il numero sia la tipologia di software malevoli che appaiono sempre più altamente sofisticati. Facilita è un applicativo web quindi esposto a potenziali attacchi (es. Sql Injection, attacco DDOS, Malware web based, Bad bot) tali da impattare anche sulla disponibilità dei dati. Tuttavia l'appetibilità dei dati è limitata e l'impatto potenziale per gli interessati può creare minime difficoltà.
Diffusione malware	**Medio**	**Basso**	**Medio**	Il malware può infiltrarsi sui sistemi informatici e le reti attraverso vari mezzi, sfruttando spesso le vulnerabilità nei software, debolezza nei protocolli di sicurezza o comportamento umano ignaro prescinde dall'appetibilità dei dati ma l'impatto potenziale per gli interessati può creare minime difficoltà.
Divulgazioni informazioni	**Medio**	**Basso**	**Medio**	La probabilità è medio-alta in quanto le divulgazioni delle informazioni possono avvenire anche inconsapevolmente.
Errore Umano	**Medio**	**Basso**	**Medio**	Il fattore umano è l'anello più debole della sicurezza e rende spesso insicura un'infrastruttura tecnologica.
Furto dispositivi	**Medio**	**Basso**	**Medio**	Il furto di dispositivi può impattare sulla disponibilità dei dati.
Furto di identità	**Medio**	**Basso**	**Medio**	Minaccia reale che può concretizzarsi in vari modi, grazie a tecniche sempre più sofisticate utilizzando

				sistemi come per esempio il phishing e malware per rubare le informazioni private degli individui.
Rischio generale per gli eventi di perdita di disponibilità	**Medio**	**Basso**	**Medio**	

Perdita di integrità	**P**	**I**	**RI**	**Motivazione**
Attacco Hacker	**Medio**	**Basso**	**Medio**	Gli attacchi cyber proliferano in maniera esponenziale poiché sono cresciuti sia il numero sia la tipologia di software malevoli che appaiono sempre più altamente sofisticati. Facilita è un applicativo web quindi esposto a potenziali attacchi (es. Sql Injection, attacco DDOS, Malware web based, Bad bot) tali da impattare anche sull'integrità dei dati. Tuttavia l'appetibilità dei dati è limitata e l'impatto potenziale per gli interessati può creare minime difficoltà.
Errore umano	**Medio**	**Basso**	**Medio**	Il fattore umano è l'anello più debole della sicurezza e rende spesso insicura un'infrastruttura tecnologica.
Malfunzionamento software	**Alto**	**Basso**	**Medio**	I difetti di un prodotto software sono sempre presenti in una certa misura e ciò non dipende da una disattenzione o irresponsabilità dello sviluppatore, ma perché la complessità del software è generalmente intrattabile e gli uomini hanno capacità limitate per gestire la complessità. Una prima tipologia di difetti che si possono presentare in un'applicazione sono quelli rilevabili da malfunzionamenti del software in fase di esecuzione, solitamente causati da difetti di design applicativo o da difetti di codice. In Facilita un bug (funzionale e di sicurezza) non rilevato, se abbastanza grave, consente a un utente malintenzionato di aggirare i controlli di accesso ealterare i dati
Manomissione software	**Medio**	**Basso**	**Medio**	La manomissione dei software può causare gravi incidenti di sicurezza. In Facilita, il verificarsi di tale

				evento minaccia appare altamente probabile e alto impatto sulla integrità del dato se non rilevata per tempo l'intromissione e la manomissione.
Rischio generale per gli eventi di perdita di integrità	**Medio**	**Basso**	**Medio**	

3.1.1. misure per gestire i rischi (art. 35, par. 7, lett. d) e considerando 90)

Come sopra riportato e come per tutte le Pubbliche amministrazioni, l'infrastruttura che ospita i dati è sottoposta alle specifiche di cui all'articolo 33-septies, comma 4, del D.L. 179/2012 e all'articolo 17, comma 6, del D.L. 82/2021 e del relativo "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione" adottato da AGID con determinazione 628/2021 e relativi atti dell'Agenzia nazionale per la cybersicurezza.

In particolare sono utilizzati servizi qualificati ACN Livello di Qualificazione almeno minimo. La qualifica assicura i criteri minimi di affidabilità e sicurezza considerati necessari per i servizi digitali pubblici. I dati trattati sono classificati quali dati "ordinari" ai sensi del regolamento citato.

Si intendono "ordinari" i dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

Al fine di garantire opportuna protezione ai dati e ai servizi strategici, critici e ordinari, il 18 gennaio 2022 l'Agenzia per la cybersicurezza nazionale, d'intesa con il Dipartimento per la trasformazione digitale, ha adottato con apposita determina n. 307/2022 le ulteriori caratteristiche dei servizi cloud e requisiti per la qualificazione.

In particolare, l'impianto si basa su un elenco di misure ispirate alle migliori pratiche e agli standard nazionali (quali ad esempio il framework nazionale di cybersecurity) e internazionali, in piena coerenza con le più recenti evoluzioni

normative in ambito cyber, in relazione al rischio e all'evoluzione della minaccia di natura cibernetica.

Per le PA che trattano dati e servizi qualificati quali ordinari, ai fini della qualificazione di livello QC1, è richiesto il rispetto delle caratteristiche di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità, di portabilità misure previste dal Regolamento AgiD e dalla Determina ACN n. 307 del 18 gennaio 2022 e ss.mm. sopra richiamate, per il livello di qualificazione richiesto a cui si rimanda per l'elenco puntuale.

Si ricorda che si è in attesa del termine del regime transitorio per la qualificazione delle infrastrutture e dei servizi cloud per le Pubbliche Amministrazioni (fissata a giugno 2024), in attesa del nuovo Regolamento unico per le infrastrutture e i servizi cloud per la PA secondo quanto previsto dalla Direttiva UE n. 2015/1535 del 9 settembre 2015 e dall' articolo 57 del regolamento UE n. 2016/679*.

Inoltre, i fornitori del DTD, in quanto fornitori di servizi cloud qualificati almeno livello QC1 (dati e servizi ordinari), possiedono almeno:

a. certificazione ISO 9001 relativa ai Sistemi di Gestione per la Qualità (SGQ)
b. certificazione ISO/IEC 27001:2013 relativa al Sistema di gestione per la sicurezza delle Informazioni(SGSI) con estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:2019
c. certificazione Cloud Security Alliance - Star Level 2

Come sopra riportato e per lo specifico servizio cloud AWS il livello di qualificazione è maggiore (QC2).

Inoltre, il DTD e i propri fornitori rispettano le disposizioni di cui al Provvedimento del 27 Novembre 2008 del Garante per la protezione dei dati personali sulle misure e accorgimenti prescritti ai titolari del trattamento effettuati con strumenti elettronici relativamente alle attribuzioni di funzioni di amministrazione di sistema e successive modifiche.

Gli accessi ai dati sono consentiti esclusivamente a dipendenti e collaboratori del DTD, appositamente autorizzati, ovvero al personale autorizzato dei responsabili del trattamento, che accedono alle risorse informative tramite doppio fattore di autenticazione e sono tracciati nelle attività di consultazione.

Alla luce delle considerazioni sopra esposte, oltre alle specifiche caratteristiche di qualità e sicurezza garantire dal livello almeno minimo di qualificazione ACN come sopra riportato' di seguito sono indicate alcune tra le principali misure di sicurezza tecniche/organizzative applicate con una descrizione specifica di implementazione in Facilita.

ID	Misura di sicurezza	Tipologia	Descrizione
1	Antimalware-Antivirus	Tecnica	Sono attuati controlli di individuazione, di prevenzione e di ripristino relativamente a malware e virus.
2	Back Up e ripristino	Tecnica	Sono adottate politiche che stabiliscono le modalità di salvataggio dei dati, inclusi i dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, nonché di recupero dei dati e ripristino dell'operatività a seguito di un evento avverso.
3	Business Continuity	Organizzativa	Sono adottate politiche atte a garantire, in caso di eventi avversi (incidente, disservizi, etc.), la disponibilità dei dati personali oggetto del trattamento. In facilità la misura di back up rappresenta un modo efficace per garantirne la continuità operativa.
4	Campagne anti-phishing	Tecnica	Sono in programma simulazioni di phishing per testare il livello di maturità degli utenti e intervenire successivamente con un piano formativo specifico in caso di esito negativo della campagna.
5	Cancellazione sicura dei dati	Tecnica	Sono adottate misure allo scopo di eliminare e distruggere irreversibilmente i dati personali quando non più necessari.
6	Controllo degli accessi logici (per la segregation of duties)	Tecnica	Sono adottate misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati, inclusi i dati personali, trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della "segregation of duties": ogni utente ha accesso ai soli dati personali strettamente

			necessari per lo svolgimento dei propri compiti.
7	Cifratura dati	Tecnica	I dati sono cifrati sia durante la permanenza nei DB o File Systems, sia durante la fase di trasporto. Una specifica misura di sicurezza relativa alla cifratura è applicata (in ambiente locale del Facilitatore) al codice fiscale del cittadino*. Il DTD non dispone di alcun accesso a basi di dati che collegano il codice fiscale di un cittadino ai dati anagrafici.
8	Firewall	Tecnica	Sono attuate regole e strumenti per la protezione dei dati personali nelle reti e nelle fasi di comunicazione attraverso l'adozione di firewall e protezioni similari.
9	Formazione del personale	Organizzativa	Sono predisposte misure specifiche per garantire che i soggetti coinvolti nel trattamento dei dati personali siano adeguatamente informati e formati in merito agli obblighi di riservatezza.
10	Gestione accessi privilegiati	Tecnica	Sono adottati processi per l'assegnazione di diritti di accesso privilegiato ai sistemi trattanti dati personali. Tali diritti di accesso sono limitati e controllati.
11	Gestione incidenti e violazioni dati personali (Data Breach)	Tecnica/organizzativa	Sono sviluppate, documentate e tenute aggiornate procedure volte alla gestione di guasti, malfunzionamenti e incidenti di sicurezza. L'accordo integrativo disciplina specificatamente le eventuali comunicazioni delle violazioni da parte dei soggetti coinvolti.
12	Gestione dei responsabili e terze parti	Organizzativa	Sono definiti i rapporti con i responsabili del trattamento e terze parti in ordine alla sicurezza delle informazioni. I fornitori sono in possesso di specifica qualifica che garantisce le misure tecniche ed organizzative idonee a a garatire la sicurezza dei dati così come disposto dalla regolamentazione AgID e ACN (si richiamano le disposizioni di cui sopra). Sono pianificati audit per verificare il possesso dei requisiti di cui alla normativa vigente in materia di cybersecurity.
13	Hardening dei sistemi IT	Tecnica	É definito ed attuato un processo di hardening dei sistemi IT. Il processo, automatizzato, appare interamente gestito dal fornitore qualificato.
14	Limitazione dei tempi di	Tecnica	Il periodo di conservazione dei dati personali è determinato in ottemperanza al principio di minimizzazione necessario per

	conservazione (data retention)		raggiungere le finalità connesse ad un determinato trattamento. A livello applicativo i dati in Facilita vengono conservati sino al termine delle verifiche UE sulla misura 1.7.2
15	Minimizzazione dei dati raccolti	Tecnica	Sono adottate misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
16	Modello organizzativo Privacy	Organizzativa	È adottato un modello organizzativo e di gestione della privacy costituente il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Tale modello viene richiesto ai fornitori e verificato dal DTD.
17	Norme e regole per lo sviluppo sicuro del codice	Tecnica	Nello sviluppo del software sono seguite le best practice di cui alle linee guida per lo sviluppo sicuro del codice adottate da AgID a garanzia del rispetto della protezione dei dati personali fin dalla progettazione e per impostazione predefinita, nel rispetto del GDPR Regolamento (UE) 2016/679 ed in linea con le indicazioni di "secure by design" e "privacy by design".
18	Politiche e procedure per la protezione dei dati personali	Organizzativa	Sono definite politiche e procedure per la protezione dei dati personali tramite accordi specifici tra i soggetti coinvolti nel trattamento nonchè tramite specifica organizzazione in materia di trattamento dati del DTD e dei fornitori.
19	Processo Patch Management	Tecnica	Processo attuato, monitorato e aggiornato per garantire la risoluzione di problemi del software e risolvere le vulnerabilità riscontrate.
20	Processo sviluppo sistema	Organizzativa	Processo definito e attuato seguendo le Linee guida AgId sull'adozione di un ciclo di sviluppo di software sicuro.
21	Raccolta e analisi dei log	Tecnica	Sono adottate misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazioni svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"),

			inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini. La misura è attuata e garantita dal fornitore qualificato ACN. In particolare, tramite il tool AWS cloudwatch, è possibile raccogliere e visualizzare tutti i dati relativi a prestazioni e operatività sotto forma di log e parametri, in un'unica piattaforma superando le problematiche di monitoraggio di singoli sistemi e applicazioni in silo (server, rete, database e così via). Consente, inoltre, di monitorare lo stack completo (applicazioni, infrastruttura e servizi) e sfruttare allarmi, log e dati relativi ad eventi per attivare operazioni automatizzate e ridurre i tempi medi di risoluzione dei problemiIl sistema.
22	Segregazione delle reti	Organizzativa	Nell'ambito del trattamento di dati personali, sono adottate tecniche in base alle quali le reti sono segregate in gruppi di servizi, di utenti e di sistemi informativi.
23	Separazione degli ambienti di sviluppo, test e produzione	Organizzativa	Gli ambienti di sviluppo, test e produzione sono separati per ridurre il rischio di accesso o cambiamenti non autorizzati ai dati personali oggetto del trattamento.
24	Sicurezza perimetrale IDS/IPS (Intrusion Detection System/ Intrusion Prevention System)	Tecnica	Sono adottati strumenti di protezione perimetrale dei sistemi trattanti dati personali, quali Intrusion Detection Systems e Intrusion Prevention Systems. Tali misure è garantita ed attuata dal fornitore qualificato ACN.
25	Strong Authentication	Tecnica	In Facilita, il processo di autenticazione diretto alla verifica dell'identità digitale degli utenti avviene: - Livello 1 corrispondente al LoA2 per tutti i profili: garantisce con un buon grado di affidabilità accertata nel corso dell'attività di autenticazione. - Livello 2 corrispondente al LoA3 per gli AdS a livello

			infrastrutturale garantisce con un alto grado di affidabilità accertata nel corso dell'attività di autenticazione. Nell'utilizzo delle identità digitali personali è escluso per impostazione predefinita l'uso dei dati personali attinenti alla sfera privata dell'operatore forniti dal Service Provider (es. e-mail e numero di cellulare personali, domicilio privato, etc.)
26	Tecniche/procedure di gestione del cambiamento (Change management)	Organizzativa	Esiste ed è attuato un processo operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ad esempio, ogni modifica è registrata e la data/orario dell'ultima modifica è conservata.
27	Test di sicurezza applicativa	Tecnica	Attuazione di Static Application Security Testing e Dinamic Application Security Testing durante la fase di progettazione del codice.
28	Vulnerability Assessment	Tecnica	É attuata e gestita la misura: in sede progettuale sono stati previsti ed effettuati cicli di Vulnerability Assessment (VA).
29	Web Application Firewall	Tecnica	Sono attuate regole e strumenti per la protezione delle applicazioni web e dei layer sottostanti comunicanti attraverso l'adozione di Web Application Firewall.
30	Anti-DDOS	Tecnica	Sono attuate regole e strumenti per la protezione dei servizi esposti attraverso l'adozione di sistemi Anti Distributed Denial of Service.
31	API-Gateway	Tecnica	Strumento dedicato alla protezione di accesso ai micro-servizi. Si attua in Facilita e vengono definiti in fase di progettazione.

3.1.2. Applicazione delle misure di mitigazione alle macrocategorie

	Perdita di riservatezza	**Perdita di disponibilità**	**Perdita di integrità**
ID.1 Antimalware/Antivirus	**x**	**x**	

ID.2 Backup e ripristino	**x**	**x**	
ID.3 Business Continuity		**x**	
ID.4 Campagne anti-phishing	**x**	**x**	
ID.5 Cancellazione sicura dei dati	**x**	**x**	
ID.6 Controllo degli accessi logici (per la segregation of duties)	**x**		**x**
ID.7 Cifratura dei dati	**x**		**x**
ID.8 Firewall	**x**	**x**	**x**
ID.9 Formazione del personale	**x**	**x**	
ID.10 Gestione degli accessi privilegiati	**x**	**x**	**x**
ID.11 Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali (Data Breach)	**x**	**x**	**x**
ID.12 Gestione dei Responsabili del trattamento e delle terze parti	**x**	**x**	**x**
ID.13 Hardening dei sistemi IT	**x**	**x**	
ID.14 Limitazione dei tempi di conservazione (Data retention)	**x**		
ID.15 Minimizzazione dei dati raccolti	**x**	**x**	
ID.16 Modello Organizzativo Privacy	**x**	**x**	**x**
ID.17 Norme e regole per sviluppo sicuro del codice	**x**	**x**	
ID.18 Politiche e procedure per la protezione dei dati personali	**x**	**x**	**x**

ID.19 Processo di patch management	x	x	
ID.20 Processo di sviluppo sistemi basato su principi di Privacy by design / Privacy by default	x	x	x
ID.21 Raccolta e analisi di log (tracciabilità)	x	x	
ID.22 Segregazione delle reti	x	x	
ID.23 Separazione degli ambienti di sviluppo, test e produzione	x	x	
ID.24 Sicurezza perimetrale IDS/IPS (Intrusion Detection System / Intrusion Prevention System)	x		
ID.25 Strong Authentication	x	x	x
ID.26 Tecniche/procedure di gestione del cambiamento (Change management)		x	
ID.27 Test di sicurezza applicativa	x	x	
ID.28 Vulnerability Assessment	x	x	
ID.29 Web Application Firewall	x	x	
ID.30 Anti-DDOS	x	x	
ID.31 API-Gateway		x	

3.1.3. Calcolo del rischio residuo

	Rischio Iniziale		Rischio Residuo
Perdita di riservatezza	**Medio**	→	**Basso**
Perdita di disponibilità	**Medio**	→	**Basso**
Perdita di integrità	**Medio**	→	**Basso**

3.1.4. Ulteriori misure in fase di programmazione

Di seguito, sono individuati gli ulteriori interventi, allo stato attuale da programmare, per rendere l'applicativo ulteriormente affidabile e sicuro.

ID.4 Campagne anti-phishing: Come noto, il phishing è uno degli strumenti più sfruttati dai cybercriminali e uno dei più efficaci nel forzare le difese di un sistema informativo. Sebbene il DTD abbia pianificato una simulazione di phishing, si dovrà programmare ad intervelli regolari (as esempio, ogni 6 mesi) delle campagne anti phishing per verificare la consapevolezza degli utenti in ambito di cybersecurity.

ID. 32 Test di sicurezza applicativa / ID 33 Vulnerability Assessment: sono stati eseguiti i test di sicurezza applicativa durante la fase di progettazione del codice. Si dovrà programmare, ad intervalli di tempo regolari e/o al verificarsi di cambiamenti importanti, test di sicurezza applicativa volti a scansionare l'applicativo con strumenti di vulnerability scanning ed effettuare penetration testing.

**La presente Valutazione di Impatto, nella sua prima versione consolidata messa a disposizione dei soggetti attuatori prima dell'attivazione della Piattaforma come previsto dall'accordo integrativo, sarà aggiornata al completamento del quadro normativo di riferimento richiamato nonchè all'esito delle interlocuzioni attualmente in corso con la Commissione Europea ai fini di consolidare gli accordi relativamente alle modalità di verifica della misura, anche per la valutazione dell'eventuale coinvolgimento delle parti interessate.*