MINISTERO del LAVORO
e delle POLITICHE SOCIALI

Allegato 4 - Metodologia per lo svolgimento della valutazione d'impatto

VALUTAZIONE DI IMPATTO

IDENTIFICAZIONE, ANALISI E GESTIONE DEL RISCHIO

Introduzione

Il presente documento ha l'obiettivo di formalizzare le risultanze della valutazione d'impatto sulla protezione dei dati eseguita dal Ministero del Lavoro e delle politiche sociali (di seguito "Ministero"), in qualità di titolare del trattamento, ai sensi e per gli effetti dell'art. 35 del Regolamento (UE) 2016/679 (di seguito "Regolamento generale sulla protezione dei dati" o, per brevità, "GDPR").

Il documento intende fornire il contesto, nonché le informazioni tecniche e di sicurezza adottate per l'acquisizione, il trattamento e l'utilizzo dei dati personali raccolti nell'ambito della [*specificare il trattamento per il quale si sta eseguendo la valutazione d'impatto*].

I primi paragrafi "Contesto normativo di riferimento" e "Funzioni relative al trattamento dei dati" si pongono l'obiettivo di descrivere, sotto il profilo del trattamento dei dati personali, finalità e funzioni dell'applicativo utilizzato e i compiti dei soggetti che vi operano, al fine di analizzare nel dettaglio le finalità, le modalità di trattamento, le categorie di dati personali dei soggetti interessati coinvolti nel trattamento e valutarne conseguentemente i rischi per i diritti e le libertà degli interessati.

Contesto normativo di riferimento

[*fornire il contesto normativo di riferimento, all'interno del quale si inserisce il trattamento in questione*].

Principi integrati nei trattamenti di dati personali eseguiti dal MLPS

I trattamenti di dati personali effettuati da MLPS sono supportati dall'utilizzo della [*specificare l'applicativo utilizzato*].

Tale strumento elettronico risulta essere stato progettato e sviluppato in conformità al principio della "Privacy by Design" di cui all'art. 25 del GDPR. In particolare, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per gli interessati, sono stati attuati i principi di protezione dei dati enunciati dalla normativa in materia di protezione dei dati personali, incluso, in particolare il Regolamento (UE) 679/2016 ("GDPR"), come da tabella sottostante:

Tabella 1 - Principi integrati nel trattamento

Principio prescritto dal GDPR	***Applicazione del principio nel [specificare la piattaforma utilizzata]***
Principio di liceità	Tutti i trattamenti eseguiti dal MLPS presentano come base giuridica l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. [*fornire un dettaglio relativamente alla base giuridica*]
Principio di trasparenza	Ai sensi degli artt. 13 e seguenti del GDPR agli interessati è fornita dal MLPS, in qualità di titolare del trattamento, per quanto di competenza, un'informativa sul trattamento dei loro dati che contiene tutte le informazioni prescritte dalla normativa in materia. [*specificare le modalità con le quali il Ministero fornisce agli interessati l'informativa*]
Limitazione delle finalità	[*Specificare la finalità del trattamento*]
Minimizzazione dei dati	I trattamenti concernono esclusivamente i dati personali sufficienti e al contempo necessari per il conseguimento delle finalità che giustificano la raccolta degli stessi.
Esattezza	[*Specificare le modalità con le quali viene assicurata l'esattezza dei dati personali trattati*].
Limitazione della conservazione	La conservazione dei dati personali è limitata al solo tempo strettamente necessario per perseguire le finalità individuate. [*specificare il periodo di conservazione dei dati personali*].
Diritti degli interessati	Al fine di garantire l'esercizio dei diritti da parte degli interessati, ai sensi degli artt. 15 e ss. del GDPR, il Ministero del Lavoro e delle Politiche Sociali ha messo a disposizione un indirizzo mail e una PEC ai quali poter inviare le istanze. Tali punti di contatto con gli interessati sono comunicati a questi ultimi all'interno della summenzionata informativa privacy.

Funzioni relative al trattamento dei dati

[*specificare le funzioni relative al trattamento dei dati, ad esempio il flusso di alimentazione dell'applicativo utilizzato, soggetti coinvolti nel trattamento etc.*]

I Profili di autorizzazione degli utenti della Piattaforma

La definizione dei profili di autorizzazione degli utenti accreditati per accedere all'applicativo è stata effettuata nella logica dell'accesso selettivo alle informazioni necessarie per il perseguimento delle specifiche finalità, nel rispetto del principio di minimizzazione sopra richiamato.

[*esplicitare i profili di autorizzazione previsti all'interno dell'applicativo utilizzato nell'ambito del trattamento in esame*].

Analisi del rischio e contro misure di sicurezza

L'attività di identificazione del rischio è stata condotta da tutti i soggetti interessati e da un gruppo di lavoro supervisionato dal RPD. La valutazione di impatto è stata eseguita per tutti quei dati che presentano un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35, paragrafo 1). In particolare, la valutazione d'impatto sulla protezione dei dati personali è stata eseguita al fine di effettuare l'identificazione delle misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La metodologia utilizzata, basata sulle "*Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)*", ha previsto dopo una fase di raccolta della documentazione della piattaforma e riesame della stessa in sedute di condivisione dedicate, l'identificazione di tutti quei rischi a cui sono esposti i dati, l'analisi del loro ciclo di vita e prendendo in considerazione il loro impiego, le finalità per cui sono utilizzati, le tecnologie impiegate e i soggetti autorizzati a trattarli.

In primo luogo, sono state ricercate le possibili fonti di rischio, che potrebbero inerire a comportamenti degli operatori o di terze parti (es: sottrazione delle credenziali, distrazione, comportamenti fraudolenti o sleali), a eventi relativi agli strumenti (es: virus informatici, malfunzionamento, intercettazioni e accessi non autorizzati) oppure a eventi relativi al contesto (es: sottrazione di strumenti contenenti dati, eventi distruttivi naturali o artificiali). In secondo luogo, sono state prese in considerazione tutte quelle ipotesi che, in generale, potrebbero implicare una violazione dei dati personali quali accessi non autorizzati, alterazione, perdita o distruzione dei dati. Infine, sono state valutate le probabilità con cui tali rischi potrebbero realizzarsi e il relativo l'impatto, assegnando per ciascun rischio individuato un livello di probabilità di realizzazione e un grado di potenziale impatto.

Una volta identificati i rischi, è stata eseguita la seconda fase del processo cioè quella che provvede alla gestione dei medesimi e, dunque, alla scelta (ove vi sia margine di valutazione) se un determinato rischio vada eliminato, mitigato oppure accettato. Tale valutazione dipende dal livello di probabilità di realizzazione del rischio e dal grado del potenziale impatto. Tale fase è ordinata altresì alla valutazione dell'adeguatezza delle garanzie e delle misure di sicurezza implementate all'interno dell'organizzazione. Ove opportuno sulla base dell'analisi dei rischi effettuata, si è proceduto alla programmazione di nuove misure di sicurezza più adeguate in relazione alle eventuali situazioni di rischio emerse (Es. sistemi di data masking).

Le garanzie e le misure di sicurezza sinora adottate dal Ministero del Lavoro a protezione dei dati personali sono:

- garanzie (adozione di tecniche di pseudonimizzazione, minimizzazione, implementazione della privacy by design e by default, previsione di procedure volte a testare, verificare e valutare l'efficacia delle garanzie e misure adottate);
- misure di sicurezza organizzative (es: norme e procedure che disciplinano l'aspetto organizzativo della sicurezza);

- misure di sicurezze fisiche (es: misure di protezione di aree, apparecchiature, dati);
- misure di sicurezza logiche (backup, piano di continuità operativa, piano di disaster recovery) sia in relazione al corretto utilizzo degli strumenti elettronici, sia in relazione alla loro gestione e manutenzione.

Le garanzie e misure di sicurezza sopra richiamate riguardano il complesso dei sistemi informativi ospitati dal Ministero.

Di seguito le misure di sicurezza tecniche che il Ministero del Lavoro intende applicare nell'ambito dell'applicativo:

- Antivirus: misure di contenimento dei virus informatici;
- Web Application Firewall;
- Intrusion detection system sia a livello applicativo che sullo strato dei dati;
- Backup dello storage dei dati;
- Tecniche di data masking statico e dinamico (pseudonimizzazione, cifratura ed audit dei dati personali);
- Tecniche di segmentazione del dato: tutte le informazioni che costituiscono la banca dati sono partizionate secondo logiche di competenza funzionale e di appartenenza territoriale degli operatori
- Tracciamento tramite log applicativi e di sistema, per il controllo sugli accessi alle applicazioni e ai dati;
- Patch Management;
- Piani di continuità operativa, nei quali sono garantiti alta affidabilità e alta disponibilità;
- Utilizzo di utenze nominative: accesso solo tramite identità digitale SPID o CIE;
- Meccanismi di autorizzazione/profilazione dell'utenza per l'accesso controllato ai dati (cfr. par. 1.5);
- Password Policy: la piattaforma non conserva nessun dato afferente alle password utente, delegando la gestione dell'identificazione utente al provider SPID o CIE.

Il processo di valutazione d'impatto si è concluso con la redazione di un report finale (presentato di seguito) che rappresenta il momento di rendicontazione delle attività svolte, in cui le informazioni precedentemente raccolte e analizzate sono state presentate in maniera sistematica e funzionale unitamente alle misure e ai rimedi elaborati e da implementare per contrastare i rischi emersi.

Sulla base delle informazioni raccolte nelle precedenti fasi relative al trattamento e alle operazioni di trattamento, al *privacy assessment* (cioè alla verifica che i principi fondamentali di trattamento siano rispettati, che siano presenti le condizioni di legittimità dello stesso e alla valutazione delle garanzie e delle misure adottate), all'identificazione, all'analisi e alla gestione dei rischi, il report seguente riporta l'indicazione specifica di:

- rischi identificati;
- valutazione del rischio inerente, ottenuta pesando il grado del potenziale impatto con la probabilità di realizzazione del rischio;
- contromisure programmate per la mitigazione dei rischi identificati;
- valutazione del rischio residuo, in esito all'adozione delle contro misure.

Report finale sulla valutazione d'impatto

Progetto per cui la valutazione d'impatto è stata condotta: [*indicare il progetto*];

Soggetti o team che ha svolto la valutazione d'impatto unitamente ai dati di contatto di un referente: [*indicare i soggetti coinvolti nello svolgimento della valutazione*];

Soggetti consultati e esito delle consultazioni: [*indicare i soggetti consultati es. DPO, Garante per la Protezione dei dati personali;*

Misure e i rimedi volti a mitigare i rischi individuati.

Al fine di poter valutare il rischio (probabilità x impatto) sono state adottate le seguenti tabelle di valutazione, mutuate dalla metodologia per l'esecuzione della Valutazione d'Impatto proposta dalla Commision Nationale de l'informatique et des libertès (CNIL) e dall'"*Handbook on Security of Personal Data Processing*" dell'Enisa:

Impatto	Valore	Descrizione
Basso	1	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	2	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	3	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).

Probabilità	Valore	Descrizione
Basso	1	Appare improbabile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (es. furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato tramite badge e codice di ingresso).
Medio	2	Appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (es. furto di supporti cartacei conservati in uffici dell'organizzazione ove l'accesso è controllato da un incaricato all'ingresso)
Alto	3	Appare estremamente facile per le fonti di rischio considerate concretizzate una minaccia basandosi sulle caratteristiche dei supporti (es. furto di supporti cartacei conservati in un locale dell'organizzazione pubblicamente accessibile)

La sintesi dei rischi individuati e delle contromisure programmate è riportata nella tabella che segue.

Rischio	Stima rischio inerente	Contromisura	Impatto (R=Riservatezza, I=Integrità, D=Disponibilità)	Stima rischio residuo
Rischio legato all'accesso improprio	Esempio: Alto (impatto alto, probabilità bassa)	Ad esempio: • Meccanismi di controllo degli accessi per restringere l'accesso alla piattaforma ai soli utenti autorizzati. • Tracciamento log sull'utilizzo della piattaforma: log applicativi e di sistema. • Meccanismi di accreditamento tramite identificazione ed autenticazione: accesso esclusivamente tramite SPID o CIE.	R	Esempio: Medio (impatto medio, probabilità bassa)

		• Sistema di profilazione: utenti non autorizzati non visualizzano nessuna informazione. • Profilazione dei sistemi informatici basato su sistemi quali API gateway su protocolli HTTPS e sistema di autenticazione basato su OAUTH 2.0 al fine di controllare gli accessi da sistemi esterni.		
Rischio di accesso da parte di non autorizzati ai dati personali e sensibili degli interessati	Esempio: Alto (impatto alto, probabilità bassa)	Ad esempio: • Gli utenti della banca dati sono profilati con profili di accesso soggetti a regole di visibilità condizionate a vincoli di competenza e/o di appartenenza territoriale (es. Servizi per il collocamento mirato provinciali). L'accesso alle informazioni personali e sensibili è regolato tramite un sistema di profilazione conforme con i principi di finalità, pertinenza, adeguatezza e non eccedenza. • Sessioni di formazione su tematiche in ambito data protection rivolte a tutto il personale coinvolto nel trattamento di dati personali.	R	Esempio: Basso (impatto basso, probabilità bassa)

Perdita delle informazioni relative alle procedure di alimentazione	Esempio: Medio (impatto medio, probabilità bassa)	Ad esempio: • Backup dei dati con policy coerenti con la dinamica della variazione dei dati in esso contenuti. Ad esempio: • Test di restore sui dati per verificare la qualità e la consistenza dei backup effettuati. • Piani di Business Continuity e di Disaster Recovery (come richiesto dall'articolo 50-bis del Codice dell'Amministrazione Digitale (CAD) al fine di garantire l'erogazione dei servizi critici in caso di prolungata indisponibilità di persone, informazioni, infrastrutture tecniche, locali/siti e servizi erogati da terze parti o processi. • Componenti di sistema ridondate o alternative al fine di garantire l'erogazione del servizio in caso di prolungata indisponibilità dell'infrastruttura IT.	R-I-D	Esempio: Basso (impatto basso, probabilità bassa)
Errata configurazione o persistenza dei permessi e profili non più pertinenti causante accesso da personale non più autorizzato	Esempio: Medio (impatto medio, probabilità bassa)	Ad esempio: • Profilazione degli utenti con meccanismo di provisioning e deprovisioning delle utenze. • Rivalidazione delle utenze sulla base delle indicazioni fornite dal Responsabile delle	R-I-D	Esempio: Basso (impatto basso, probabilità bassa)

		Utenze per ciascun Ufficio/servizio.		
Perdita dei dati per fault hardware o per procedura errata da parte degli amministratori	Esempio: Alto (impatto alto, probabilità bassa)	Ad esempio: • Backup effettuati con cadenza giornaliera su data center ed infrastruttura di business continuity. • I servizi infrastrutturali previsti dal Piano di Continuità Operativa adottato dal MLPS.	I-D	Esempio: Medio (impatto medio, probabilità bassa)
Rischio di corruzione o sottrazione dei dati dovuto a virus informatici/cryptolocker (Disservizio al cliente o abuso da parte di terzi con perdita di riservatezza per gli interessati)	Medio (impatto medio, probabilità bassa)	Ad esempio: • Presenza di Anti-virus e anti-malware in grado di proteggere la piattaforma da tutte le forme di software malevolo. • Web Application Firewall. • Intrusion detection system, sia a livello applicativo che sullo strato dei dati.	R-I-D	Basso (impatto basso, probabilità bassa)
Rischio di divulgazione delle informazioni relative a utenti, sistemi, incidenti sui sistemi.	Esempio: Medio (impatto medio, probabilità bassa)	Ad esempio: • Profilazione degli utenti che accedono al sistema. • Formazione agli operatori sull'importanza dei dati gestiti dal sistema. • Sviluppo della consapevolezza degli operatori che svolgono assistenza.	R	Esempio: Basso (impatto basso, probabilità bassa)
Rischio di cancellazione involontaria / dolosa da parte di operatori amministratori di sistema	Esempio: Medio (impatto medio,	Ad esempio: • Backup dei dati con policy coerenti con la dinamica della variazione dei dati in esso contenuti.	I-D	Esempio: Basso (impatto basso, probabilità bassa)

	probabilità bassa)	• I servizi infrastrutturali previsti dal Piano di Continuità Operativa adottato dal MLPS.		
Rischio di defacement del sito web	Esempio: Alto (impatto alto, probabilità bassa)	Ad esempio: • La piattaforma non conserva nessun dato afferente alle password utente, delegando la gestione dell'identificazione utente al provider SPID o CIE. • Web Application Firewall. • Intrusion detection system, sia a livello applicativo che sullo strato dei dati.	I-D	Esempio: Medio (impatto medio, probabilità bassa)