MLPS, DM 6 maggio 2025, n. 60 - Disciplina degli elementi essenziali del trattamento dei dati personali di cui all'art. 4, c. 2, del DM 170/2024 - implementazione del Portale nazionale del sommerso

Il Ministro del Lavoro e delle Politiche Sociali

VISTO il Regolamento (UE) 2020/2094 del Consiglio del 14 dicembre 2020, che istituisce uno strumento dell'Unione europea a sostegno della ripresa dell'economia dopo la crisi conseguente alla pandemia da COVID-19;
VISTO il Regolamento (UE) 2021/241 del Parlamento Europeo e del Consiglio del 12 febbraio 2021, che istituisce il dispositivo per la ripresa e la resilienza;
VISTA la decisione del Consiglio ECOFIN del 13 luglio 2021, recante l'approvazione della valutazione del Piano per la ripresa e la resilienza dell'Italia e notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021;
VISTO il Regolamento delegato (UE) 2021/2106 della Commissione del 28 settembre 2021, che integra il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio, che istituisce il dispositivo per la ripresa e la resilienza, stabilendo gli indicatori comuni e gli elementi dettagliati del quadro di valutazione della ripresa e della resilienza;
VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
VISTO il documento Recovery and resilience facility - Operational Arrangements between the European Commission and Italy – Ref. Ares (2021) 7047180-22/12 2021 (OA), relativo al Piano Nazionale di Ripresa e Resilienza dell'Italia sottoscritto in data 22 dicembre 2021;
VISTO il decreto-legge 31 maggio 2021, n. 77, concernente "Governance del Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure", convertito, con modificazioni, dalla legge 29 luglio 2021, n. 108;
VISTO il decreto del Presidente del Consiglio dei ministri 9 luglio 2021, recante l'individuazione delle amministrazioni centrali titolari di interventi previsti dal PNRR ai sensi del richiamato articolo 8, comma 1, del decreto-legge 31 maggio 2021, n. 77;
VISTI i traguardi e gli obiettivi che concorrono alla presentazione delle richieste di rimborso semestrali alla Commissione europea, ripartiti per interventi a titolarità di ciascuna Amministrazione, riportati nella Tabella B allegata al decreto del Ministero dell'economia e delle finanze del 6 agosto 2021 e successive modificazioni;
VISTO il decreto del Ministero del lavoro e delle politiche sociali del 19 dicembre 2022, n. 221, con cui è stato adottato il Piano nazionale per la lotta al lavoro sommerso per il triennio 2023-2025;
VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
VISTO il decreto legislativo 23 aprile 2004, n. 124 recante "Razionalizzazione delle funzioni ispettive in materia di previdenza sociale e di lavoro, a norma dell'articolo 8 della legge 14 febbraio 2003, n. 30", come modificato dal decreto-legge 30 aprile 2022, n. 36, recante "Ulteriori misure urgenti per l'attuazione del Piano nazionale di ripresa e resilienza", convertito, con modificazioni, dalla legge 29 giugno 2022, n. 79;
VISTO, in particolare, l'articolo 10, comma 1, del decreto legislativo 23 aprile 2004, n. 124, secondo il quale "al fine di una efficace programmazione dell'attività ispettiva nonché di monitorare il fenomeno del lavoro sommerso su tutto il territorio nazionale, le risultanze dell'attività di vigilanza svolta dall'Ispettorato nazionale del lavoro e dal personale ispettivo dell'INPS, dell'INAIL, dell'Arma dei Carabinieri e della Guardia di finanza avverso violazioni in

materia di lavoro sommerso nonché in materia di lavoro e legislazione sociale confluiscono in un portale unico nazionale gestito dall'Ispettorato nazionale del lavoro denominato Portale nazionale del sommerso (PNS). Il Portale nazionale del sommerso sostituisce e integra le banche dati esistenti attraverso le quali l'Ispettorato nazionale del lavoro, l'INPS e l'INAIL condividono le risultanze degli accertamenti ispettivi";
VISTO, altresì, il comma 1-bis del predetto articolo 10 secondo cui "nel portale di cui al comma 1 confluiscono i verbali ispettivi nonché ogni altro provvedimento consequenziale all'attività di vigilanza, ivi compresi tutti gli atti relativi ad eventuali contenziosi instaurati sul medesimo verbale";
VISTO il decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, concernente "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
VISTO il decreto legislativo 18 maggio 2018, n. 51, di "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";
VISTO il decreto legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE ("Regolamento generale sulla protezione dei dati");
VISTO il decreto ministeriale n. 170 del 20 novembre 2024 avente ad oggetto l'implementazione del Portale nazionale del sommerso;
VISTO, altresì, l'articolo 4, comma 2, del predetto decreto ministeriale che, recependo le osservazioni formulate dal Garante per la protezione dei dati personali con il provvedimento n. 723 del 18 novembre 2024, rinvia all'adozione di un successivo decreto del Ministro del lavoro e delle politiche sociali, da adottarsi ai sensi dell'articolo 10, comma 1-ter, del decreto legislativo 23 aprile 2004, n. 124, al fine di disciplinare più dettagliatamente gli elementi essenziali del trattamento;
SENTITO l'Ispettorato Nazionale del Lavoro, l'INPS e l'INAIL;
SENTITO il Garante per la protezione dei dati personali;

DECRETA

Articolo 1

(Tipologie di dati personali trattati dal Portale nazionale del sommerso)

1. Le tipologie di dati personali trattati all'interno del Portale nazionale del sommerso (di seguito anche Portale o PNS) sono dettagliate nel tracciato dati di cui all'allegato A).
2. Nell'allegato A) sono indicati anche i dati provenienti dalla Piattaforma per la gestione delle azioni di compliance e per il contrasto al lavoro sommerso di INPS.
3. I dati sono conferiti e consultati da INL, INPS, INAIL, Arma dei Carabinieri e Guardia di Finanza soggetti cooperanti ai sensi dell'articolo 10, comma 1, del decreto legislativo 23 aprile 2004, n. 124.
4. Con successivi protocolli di intesa da stipulare ai sensi dell'articolo 1, comma 2, del D.M. 20 novembre 2024, n. 170, sono individuati i documenti oggetto di condivisione che non sono caricati né transitano sul Portale nazionale del sommerso, restando nella esclusiva disponibilità dei soggetti cooperanti che li hanno formati. L'accesso agli stessi sarà successivamente richiesto direttamente ai rispettivi soggetti cooperanti attraverso canali esterni utilizzando specifiche funzionalità da implementare all'interno del Portale.
5. Il trattamento dei dati raccolti nel Portale avviene nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione dei dati, integrità e riservatezza.

Articolo 2

(Ruolo dei soggetti coinvolti nel trattamento)

1. I soggetti cooperanti alimentano il Portale nazionale del sommerso assumendo il ruolo di Titolari autonomi del trattamento, assicurando la correttezza, l'esattezza e l'aggiornamento dei dati e rendendo agli interessati, ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016,

le rispettive informative sul trattamento dei dati personali.
2 .L'INL assume il ruolo di Titolare del trattamento dei dati raccolti e trattati all'interno del PNS e garantisce la gestione tecnica ed informatica del PNS ospitato sulla sua infrastruttura cloud.

Articolo 3
(Misure tecniche e organizzative per garantire livelli di sicurezza adeguati)

1. Lo scambio dei dati avviene mediante gli appositi servizi pubblicati nel catalogo della Piattaforma Digitale Nazionale Dati (PDND), nel rispetto delle disposizioni normative vigenti in materia di protezione dei dati personali e interoperabilità dei sistemi informativi della Pubblica Amministrazione.
2. Per garantire adeguati livelli di sicurezza, la continuità operativa del sistema e la protezione dei dati nell'ambito del Portale nazionale del sommerso, l'Ispettorato nazionale del lavoro adotta misure tecniche e organizzative in conformità alle disposizioni del Regolamento (UE) 2016/679 (GDPR), del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), come dettagliate nell'allegato B) che costituisce parte integrante del presente decreto.
3. Ciascun soggetto cooperante è responsabile dell'adozione di idonee misure tecniche e organizzative ai fini del corretto trattamento dei dati di cui all'articolo 1 del presente decreto sui rispettivi sistemi, nonché del corretto utilizzo dei dati acquisiti tramite il Portale nel rispetto delle normative sulla protezione dei dati personali e delle misure di sicurezza come dettagliate nell'allegato C) che costituisce parte integrante del presente decreto
4. L'accesso ai dati del Portale è consentito esclusivamente ai soggetti abilitati, secondo profili autorizzativi definiti da ciascun soggetto cooperante in base alle rispettive competenze istituzionali e alle finalità perseguite nel rispetto delle misure di cui all'Allegato C).
5. Ogni soggetto cooperante è tenuto a segnalare tempestivamente all'INL ogni incidente di sicurezza che possa aver comportato una compromissione della integrità, riservatezza e disponibilità dei dati trattati dal Portale nazionale del sommerso in modo che, nei termini prescritti, ogni titolare possa effettuare gli adempimenti di cui agli articoli 33 e 34 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. L'INL, in qualità di titolare del trattamento per la gestione informatica e tecnica del PNS, comunica al soggetto cooperante gli incidenti di sicurezza che lo possano interessare, ai fini dei prescritti adempimenti di cui al capoverso precedente.
6. È fatto divieto ai soggetti cooperanti di duplicare la banca dati presso i propri sistemi anche avvalendosi di sistemi automatici di interrogazione.

Articolo 4
(Tempi di conservazione)

1. I dati trattati nell'ambito del Portale nazionale del sommerso, riferiti a ciascun fascicolo inerente accertamenti ispettivi e di compliance, sono conservati per cinque anni decorrenti dalla data di acquisizione dell'ultima informazione o atto pertinente allo stesso fascicolo, decorsi i quali i predetti dati vengono cancellati.

Articolo 5
(Modifiche e integrazioni)

1. Il presente provvedimento potrà essere oggetto di modifiche e integrazioni che incidono su aspetti essenziali del trattamento dei dati personali, previa consultazione del Garante per la protezione dei dati personali. Resta ferma la possibilità di regolare aspetti di dettaglio anche mediante i protocolli d'intesa di cui all'articolo 1, comma 2, del D.M. 20 novembre 2024, n. 170.

Articolo 6
(Clausola di invarianza finanziaria)

1. Le Amministrazioni provvedono alle attività di cui al presente decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri a carico della finanza pubblica.
Il presente decreto sarà pubblicato sul sito internet istituzionale del Ministero del lavoro e delle politiche sociali all'indirizzo: www.lavoro.gov.it – sezioni "Pubblicità legale" e "Normativa".

Roma, *6 maggio 2025*

IL MINISTRO
DEL LAVORO E DELLE POLITICHE SOCIALI

Marina Elvira Calderone

Allegato A

Misure di sicurezza tecniche e operative implementate sui sistemi informatici INL

Misure di sicurezza relative al sistema di gestione delle identità

- Impiego del Tier model;
- Segregazione delle utenze con privilegi amministrativi;
- Utilizzo di sistemi di Privileged Identity Management (PIM) per le utenze amministrative per elevazione dei privilegi in modalità Just In Time (JIT), con processo di approvazione delle richieste;
- Criteri di robustezza minima delle password;
- Conservazione delle password mediante sistemi di cifratura non reversibile;
- Utilizzo di sistemi di analisi automatica dei profili di rischio associati alle utenze e identificazione automatica di pattern anomali;
- Sistemi di strong authentication (MFA) per l'accesso online di tutti i ruoli con privilegi amministrativi e per l'accesso a tutti i portali di amministrazione dei servizi;
- Sistemi di strong authentication (MFA) per l'accesso da rete esterna a tutti i sistemi e servizi INL da parte di tutti gli utenti INL;

Misure di sicurezza a livello network

- Sistemi di sicurezza perimetrale a protezione della rete e dei sistemi in Cloud;
- Implementazione web filtering profiles a protezione della navigazione web;
- Monitoraggio continuo della rete;

Misure di sicurezza per le postazioni di lavoro e per l'accesso ai servizi:

- Protezione delle postazioni di lavoro tramite sistemi antivirus/antimalware;
- Installazione automatica periodica e tempestiva per gli aggiornamenti e patch di sicurezza;
- Utilizzo di sistemi XDR integrati in tutte le postazioni di lavoro:

o Protezione avanzata contro le minacce informatiche agli endpoint in tempo reale
o Individuazione tempestiva di eventuali minacce avanzate e violazioni della sicurezza
o Integrazione con sistema SIEM;
o Reportistica dettagliata sulle potenziali attività malevole sulle postazioni di lavoro degli utenti e sulle minacce informatiche

- Protezione del sistema di posta elettronica:

o Sistema antispam/antiphishing
o Sistema safe-link;
o Sistema sand-box per analisi degli allegati;
o Monitoraggio minacce;

- Utilizzo di sistemi integrati per la sicurezza dei servizi SaaS di business productivity in Cloud;
- Protezione da perdita di dati per guasto della postazione di lavoro: mediante l'impiego di sistemi di storage in cloud;
- Segregazione tra "area di lavoro" e "area personale" sui device mobili in uso al personale, con possibilità di cancellazione da remoto in caso di furto o smarrimento;
- Sistema di gestione dei device aziendali per garantire la distribuzione di aggiornamenti e patch di sicurezza e la conformità alle policy di sicurezza predefinite;
- Sistemi di strong authentication, conditional access e risk based access policy:

o Autenticazione a due fattori (MFA) per tutti i ruoli amministrativi, nonché per l'accesso a tutti i portali di amministrazione dei sistemi;
o Autenticazione a due fattori (MFA) per gli accessi dall'esterno della rete INL per tutti gli utenti su tutti i sistemi e servizi online dell'Amministrazione;
o Blocco degli accessi da IP esteri, per prevenire attacchi da aree geografiche a rischio; in caso di motivata richiesta, specifici utenti possono essere abilitati all'accesso da IP esteri limitatamente al tempo strettamente necessario;

o Analisi dei login a rischio (risky login): sulla base di analisi automatiche, il sistema forza un nuovo login con richiesta di MFA nel caso in cui il pattern utente venga classificato a rischio medio/alto;
o Analisi degli utenti a rischio (risky users): sulla base di analisi automatiche, il sistema forza cambio password e relogin con MFA nel caso in cui un utente venga classificato come a rischio medio/alto di compromissione;

Misure di sicurezza per l'infrastruttura di cloud computing

- Utilizzo di sistemi SIEM per il monitoraggio continuo dei sistemi;
- Impiego di sistemi API gateway a protezione di specifici servizi;
- Servizio di Threat intelligence;
- Servizio SOC/NOC;
- Cifratura delle connessioni e cifratura dei dati "at rest";
- Log degli accessi e delle operazioni;
- Utilizzo del sistema Privileged Identity Managment per accesso just-in-time per le utenze con ruoli amministrativi in cloud;
- accesso con MFA per tutti i ruoli amministrativi in cloud e per l'accesso a tutti i portali amministrativi;
- Utilizzo di utenze cloud only non sincronizzate on premise per i ruoli amministrativi in cloud (configurate per uso di PIM JIT e MFA);
- Protezione da attacchi esterni mediante sistemi di DDOS Protection ed External Attack Surface Management (EASM);
- Protezione delle risorse, sistemi e servizi in cloud tramite sistemi integrati di rilevamento automatico e protezione;
- Protezione della BRAND Reputation mediante monitoraggio dei report DKIM e DMARC per identificare eventuali tentativi di uso improprio del dominio di posta elettronica dell'Amministrazione;
- Sistema automatico di backup dei dati e dei sistemi;
- Ridondanza dei sistemi e delle risorse per alta affidabilità dei servizi;

Misure organizzative:

- Processo di gestione del ciclo di vita delle utenze;
- Processo di ricognizione periodica delle utenze in uso a fornitori esterni;
- Processo di gestione degli alert di sicurezza ed incident management tramite SOC;
- Formazione periodica e awareness del personale in ambito protezione dati e sicurezza informatica;
- Esecuzione periodica di assessment di sicurezza e implementazione remediation sui sistemi dell'Amministrazione;
- Adozione dei framework "security by design" e "privacy by design";

Allegato C
Misure tecniche e organizzative da implementare da parte dei Soggetti cooperanti

Con riguardo alle modalità di accesso, ciascun Soggetto cooperante, nell'ambito di rispettiva competenza, in riferimento ai propri sistemi informativi ed in ragione dei trattamenti di dati rispettivamente effettuati, adotta adeguate misure tecniche e organizzative di sicurezza, atte a realizzare una idonea postura di sicurezza dei propri sistemi, nonché a garantire integrità, riservatezza e disponibilità dei dati nel rispetto della vigente normativa in materia di protezione dei dati personali.

Misure Generali

I soggetti cooperanti adottano misure tecniche e organizzative sui propri sistemi informatici atte a garantire una idonea postura di sicurezza complessiva, ed in particolare:
- consentono l'accesso ai dati esclusivamente ai soggetti incaricati di svolgere le attività di controllo nell'ambito delle proprie attività istituzionali. A tal fine, agli stessi dipendenti autorizzati al trattamento a norma dell'articolo 32, paragrafo 4, del Regolamento (UE) n. 2016/679 dovranno essere fornite istruzioni di sicurezza che abbiano ad oggetto non già la sola implementazione delle misure di sicurezza di cui all'articolo 32 del Regolamento, ma anche delle misure idonee, ossia di tutte le attività e le condotte utili a garantire un livello di protezione per i dati personali adeguato al rischio in relazione al contesto specifico;
- adottano sistemi di profilazione degli utenti atti a garantire l'accesso ai dati solo da parte del personale abilitato;

- implementano processi di gestione del ciclo di vita delle utenze atti a garantire la tempestiva disattivazione/deprofilazione delle utenze non più autorizzate all'accesso;
- implementano idonei criteri di adeguata robustezza delle password, che devono essere diligentemente custodite dagli utenti;
- implementano sistemi di autenticazione a più fattori (MFA);
- adottano sistemi di protezione da virus e malware sulle postazioni di lavoro in uso al personale;
- adottano sistemi per l'aggiornamento delle postazioni di lavoro in uso al personale, atti a garantire la tempestiva installazione di aggiornamenti e patch di sicurezza, nonché il costante aggiornamento dei sistemi antivirus e antimalware;
- adottano sistemi di sicurezza fisica dei locali ove si trovano le postazioni di lavoro del personale e/o copie cartacee delle pratiche in lavorazione;
- adottano sistemi di sicurezza perimetrale per le proprie reti informatiche e per i propri datacenter, atti a prevenire accessi esterni non autorizzati o altre tipologie di attacchi che impattino sulla riservatezza, integrità e disponibilità dei dati trattati;
- implementano sistemi di backup dei dati e/o di cloud storage atti a garantire integrità e disponibilità degli stessi;
- adottano sistemi di cifratura dei dati sui dispositivi portatili in uso agli utenti;
- effettuano una formazione periodica degli utenti in materia di sicurezza informatica, protezione dei dati, buone pratiche per l'uso delle tecnologie, dispositivi e sistemi informatici durante lo svolgimento delle attività lavorative;
- forniscono idonee indicazioni di sicurezza agli utenti in regime di lavoro agile e/o per l'uso di dispositivi di proprietà dell'utente (BYOD).

Misure specifiche per l'accesso al PNS

L'accesso avviene in cooperazione applicativa mediante i servizi appositamente predisposti e pubblicati in PDND. A tal fine, i soggetti cooperanti:
- inviano al PNS, per il tramite dei servizi di cooperazione applicativa, il codice fiscale dell'operatore che ha effettuato l'interrogazione;
- nelle more delle attività di aggiornamento dei propri sistemi per adempiere al punto precedente, implementano specifici sistemi di logging per tracciare: utente che effettua l'interrogazione; Codice Fiscale dell'impresa per la quale si effettua l'interrogazione; data in cui è stata effettuata l'interrogazione;

Misure ulteriori per l'accesso ai dati di tipo giudiziario

Al fine di garantire un ulteriore livello di protezione per i dati di tipo giudiziario presenti nel PNS, i soggetti cooperanti:
- implementano nei propri cruscotti di visualizzazione dei dati PNS sistemi che prevedano la visualizzazione del dato giudiziario solo a seguito di specifica ulteriore richiesta dell'utente, con inserimento obbligatorio della motivazione della consultazione;
- inviano la motivazione indicata al PNS per il tramite dei servizi di cooperazione applicativa

Conservazione dei log

Al fine di consentire un adeguato monitoraggio degli accessi al PNS e delle operazioni effettuate sui dati ivi disponibili, i log relativi al tracciamento dei login e delle interrogazioni effettuate dagli utenti autorizzati sono conservati per 24 mesi da parte di tutti i soggetti cooperanti.