Il Ministro del Lavoro e delle Politiche Sociali

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali*";

VISTO il decreto del Presidente del Consiglio dei ministri 20 gennaio 2015, n. 77, recante "*Regolamento di organizzazione degli Uffici di diretta collaborazione del Ministro del lavoro e delle politiche sociali e dell'Organismo indipendente di valutazione della performance*";

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 (di seguito, per brevità, "Regolamento"), divenuto direttamente applicabile il 25 maggio 2018;

VISTO il decreto del Presidente della Repubblica 15 marzo 2017, n. 57, recante *"Regolamento di organizzazione del Ministero del lavoro e delle politiche sociali";*

VISTO il decreto legislativo 15 settembre 2017, n. 147, recante "*Disposizioni per l'introduzione di una misura nazionale di contrasto alla povertà*";

VISTO il decreto del Ministro del Lavoro e delle Politiche Sociali *pro tempore* 6 dicembre 2017 recante "*Individuazione delle unità organizzative di livello dirigenziale non generale nell'ambito del Segretariato generale e delle Direzioni generali* ";

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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*";

VISTO il decreto del Ministro del lavoro e delle politiche sociali *pro tempore* n. 37 del 10 aprile 2019, recante "*Direttiva per la individuazione dei soggetti tramite i quali il Ministero del Lavoro e delle Politiche Sociali esercita le funzioni di titolare del trattamento, ai sensi del regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*";

VISTO il decreto del Presidente del Consiglio dei ministri 24 giugno 2021, n. 140, pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 241 dell'8 ottobre 2021, recante "Regolamento concernente modifiche al regolamento di organizzazione del Ministero del lavoro e delle politiche sociali";

VISTO il decreto del Presidente della Repubblica del 21 ottobre 2022, pubblicato nella Gazzetta Italiana della Repubblica Italiana n. 250 del 25 ottobre 2022, recante "*Nomina dei Ministri*", ivi compresa quella del Ministro del lavoro e delle politiche sociali Dott.ssa Marina Elvira Calderone;

CONSIDERATO che il Ministero del lavoro e delle politiche sociali ha provveduto a designare un Responsabile della protezione dei dati (di seguito, per brevità, anche "RPD"), ai sensi e per gli effetti dell'art. 37 del Regolamento (UE) 2016/679 assegnando allo stesso tutti i compiti previsti dall'art. 39 del Regolamento sopracitato;

VISTO il proprio decreto n. 253 del 29 dicembre 2021, con il quale, ai sensi e per gli effetti del citato decreto del Presidente del Consiglio dei ministri n. 140/2021, sono stati modificati gli articoli 3 (Soggetti che

esercitano le funzioni di titolare del trattamento dei dati personali) e 13 (Formazione del personale) del decreto del Ministro del lavoro e delle politiche sociali *pro tempore* n. 37/2019;

VISTA la Direttiva recante misure tecniche e organizzative inerenti alla protezione dei dati personali ai sensi dell'articolo 24 del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, adottata in data 29 dicembre 2021;

CONSIDERATA l'opportunità di procedere a una revisione della Direttiva sopra richiamata, atteso il percorso intrapreso dal Ministero del lavoro e delle politiche sociali volto a un costante adeguamento alla normativa tempo per tempo vigente e a un miglioramento ed efficientamento continuo delle misure e degli strumenti adottati dall'Amministrazione in materia di protezione dei dati personali;

RITENUTO di procedere all'adozione della Direttiva in argomento;

EMANA

la seguente

DIRETTIVA RECANTE MISURE TECNICHE E ORGANIZZATIVE INERENTI ALLA PROTEZIONE DEI DATI PERSONALI AI SENSI DELL'ART. 24 DEL REGOLAMENTO (UE) 2016/679, RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÈ ALLA LIBERA CIRCOLAZIONE DI TALI DATI.

Art. 1
(Premesse)

La presente Direttiva, adottata ai sensi dell'art. 24 del Regolamento (UE) 2016/679 (di seguito GDPR), si applica ai dati personali trattati dal Ministero del Lavoro e delle Politiche Sociali e ha lo scopo di definire, nell'ambito dell'organizzazione del Ministero, specifiche responsabilità a vari livelli, finalizzate a garantire la conformità al GDPR relativamente ai trattamenti di cui l'Amministrazione è titolare.

L'adozione di tale atto avviene in coerenza con quanto prescritto nel DM n. 37 del 10 aprile 2019 (Direttiva per la individuazione dei soggetti tramite i quali il Ministero del Lavoro e delle Politiche Sociali esercita le funzioni di titolare del trattamento, ai sensi del regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e successive modificazioni, il quale definisce l'assetto organizzativo, in termini di ruoli e responsabilità, in relazione ai trattamenti di dati personali da parte dell'Amministrazione, e ha l'obiettivo di specificare e descrivere le misure adottate dal Ministero del Lavoro e delle Politiche Sociali, anche sulla base di quanto stabilito nella succitata Direttiva del 2019.

La Direttiva ha, altresì, lo scopo di sistematizzare in un unico documento tutte le attività e tutti gli atti adottati dall'Amministrazione (es. linee guida, procedure, standard di nomine etc.) in ottemperanza agli adempimenti previsti in capo al Titolare del Trattamento e in coerenza con il principio di *Accountability*

(responsabilizzazione) per cui il Titolare deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative e tecniche per la protezione dei dati personali.

L'adozione di tale documento si pone in continuità con il percorso di adeguamento intrapreso da tempo dal Ministero e volto a mettere in sicurezza i trattamenti di dati personali effettuati nell'esercizio dei propri compiti istituzionali, in ossequio a quanto previsto dalla normativa vigente in materia.

Gli allegati al presente atto, da intendersi parte integrante e sostanziale della Direttiva, al fine di fornire una rappresentazione fedele delle iniziative condotte dall'Amministrazione, saranno oggetto di periodico aggiornamento in base agli ulteriori atti/documenti adottati dal Ministero e alle eventuali evoluzioni normative che interverranno.

Art. 2

(Gestione dei contratti e delle convenzioni che prevedono trattamenti e scambio di dati)

I soggetti esercenti le funzioni di titolare del trattamento, nel regolare i rapporti con terze parti, provvedono, ciascuno per la parte di propria competenza, a formalizzare esplicitamente e adeguatamente tutti gli aspetti relativi alla protezione dei dati personali.

In particolare, laddove la convenzione/protocollo preveda l'affidamento di prestazioni di pertinenza del Ministero o attività connesse, o strumentali e di supporto a terze parti, che comportino il trattamento di dati personali, l'esercente le funzioni di titolare del trattamento provvede a designare i soggetti esterni a cui sono affidate tali attività quali Responsabili del trattamento, in conformità a quanto previsto dall'art. 28 del Regolamento (UE) 2016/679. Per la nomina a responsabile, il soggetto deve presentare garanzie sufficienti e l'accertamento di tali garanzie deve essere documentato, tenendo presente che Titolare e Responsabile del trattamento assumono in solido (art. 82 del GDPR) le responsabilità di danni cagionati agli interessati. La nomina a responsabile del trattamento è un atto contrattuale (art. 28 del GDPR) che può essere incorporato nel contratto di fornitura o in un articolo della convenzione, oppure configurarsi come allegato che ne rappresenta comunque un'estensione e quindi firmato dall'esercente le funzioni di titolare del trattamento. Viceversa, nel caso in cui sia il Ministero a trattare i dati personali per conto della terza parte, ai sensi del succitato art. 28 del GDPR, l'Amministrazione dovrà essere nominata responsabile del trattamento nei termini su rappresentati.

Laddove il Ministero determini congiuntamente con una terza parte le finalità e i mezzi del trattamento, è necessario, ai sensi dell'art. 26 del GDPR, provvedere alla formalizzazione di un accordo di contitolarità all'interno del quale vengano specificate le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informative privacy.

Nell'ipotesi in cui il Ministero e la terza parte trattino per effetto di una convenzione o contratto dati personali, definendone ciascuna parte le proprie finalità e modalità di trattamento, il rapporto di autonoma

titolarità deve essere formalizzato all'interno della convenzione o accordo, unitamente all'impegno di ciascuna parte a rispettare la normativa vigente in materia di protezione dei dati personali.

Ciascun esercente le funzioni di titolare del trattamento che gestisce contratti e/o convenzioni che comportano trattamenti e/o scambio di dati personali ai sensi del GDPR:

a) verifica che le organizzazioni e i fornitori individuati, che si configurano come responsabili esterni del trattamento, presentino garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate, in modo che il trattamento soddisfi i requisiti del GDPR;
b) in caso di convenzioni che prevedano scambio di dati, valuta accuratamente la rispondenza ai principi del GDPR e in particolare alle condizioni di liceità del trattamento e alle esigenze di minimizzazione dei dati personali;
c) provvede, ove necessario, all'atto di nomina dei responsabili del trattamento utilizzando lo standard di nomina a responsabile del trattamento, allegato alla presente procedura.

Nell'esecuzione di tali adempimenti relativi alla gestione dei rapporti con le terze parti, gli esercenti le funzioni di titolare del trattamento utilizzano gli standard di convenzione (Allegato 1) e di nomina a responsabile del trattamento (Allegato 2), allegati alla presente Direttiva.

Art. 3

(Gestione del registro delle attività di trattamento)

Il Registro delle attività di trattamento del Ministero è stato sistematizzato all'interno di un *software*, allo scopo di renderlo uno strumento di gestione dei rischi e degli adempimenti in materia di tutela dei dati personali più agile ed efficace, facilitandone, altresì, la tenuta e il suo costante aggiornamento.

I soggetti individuati per l'esercizio delle funzioni di titolare del trattamento, con il supporto dei responsabili interni del trattamento e dei referenti privacy, provvedono all'aggiornamento del Registro, ai sensi dell'art. 30 del Regolamento, ogniqualvolta dovessero intervenire delle modifiche ai trattamenti (es. nuovo trattamento, variazione del supporto utilizzato per la conservazione dei dati, cessazione di un trattamento etc.), ciascuno con riferimento ai trattamenti di propria competenza.

Ciascun esercente le funzioni di titolare del trattamento, in relazione ai trattamenti di propria competenza:

- assicura la liceità e il rispetto dei principi del GDPR;
- pone particolare attenzione a informazioni quali il periodo di conservazione dei dati, la presenza di dati di minori, il trasferimento dei dati verso paesi terzi e alle relative prescrizioni previste dal GDPR.

Il Registro viene messo a disposizione dell'Autorità Garante per la protezione dei dati personali, in caso di specifiche richieste o ispezioni.

L'aggiornamento del Registro, in termini di periodicità e modalità di intervento, avviene in conformità a

quanto previsto all'interno della "Procedura di gestione del Registro delle attività di trattamento" (Allegato 3).

Art. 4

(Analisi del rischio)

Il Titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio per ciascun trattamento di dati personali svolto, ai sensi dell'art. 32 del Regolamento (UE) 2016/679.

Gli esercenti le funzioni di titolare del trattamento, in base a quanto prescritto dal DM 37 del 10 aprile 2019 e ss.mm.ii., con il supporto dei referenti privacy, ciascuno per i trattamenti di propria competenza, sono tenuti a valutare l'adeguato livello di sicurezza, tenendo in considerazione i rischi presentati dal trattamento che derivano, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Tale analisi si traduce nella valutazione dell'impatto e della probabilità del verificarsi di possibili minacce per i diversi trattamenti dei dati personali svolti da parte dell'Amministrazione.

L'analisi del rischio è inserita e gestita all'interno del *tool* del Registro dei trattamenti, attraverso l'istituzione di un'apposita sezione dedicata alla conduzione della valutazione in oggetto, sempre in un'ottica di digitalizzazione ed efficientamento dell'Amministrazione.

Al fine di condurre la valutazione dell'analisi del rischio, ciascun esercente le funzioni di titolare del trattamento è tenuto a comprendere e valutare i seguenti aspetti:

1. le operazioni di trattamento e il contesto nell'ambito del quale le stesse sono attuate;
2. l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche derivanti dalla possibile perdita di sicurezza dei dati personali;.
3. le minacce correlate al contesto del trattamento e valutare la loro probabilità di accadimento;
4. il rischio inerente, ottenuto sulla base delle valutazioni di impatto dell'operazione di trattamento dei dati personali e della probabilità di accadimento delle minacce prese in considerazione;
5. l'adeguatezza delle misure di sicurezza implementate a tutela dei dati personali;
6. il livello di rischio finale, calcolato tenendo in considerazione le misure di sicurezza adottate in un'ottica di protezione dei dati personali (c.d. residuo).

A valle dell'analisi svolta, ciascun esercente le funzioni di titolare del trattamento sarà chiamato a mettere in atto le misure di sicurezza di propria competenza ritenute non adeguatamente implementate al fine di rafforzare le stesse, formulando un piano di azione, da condividere con il RPD al fine di recepire eventuali osservazioni.

L'Analisi del rischio dovrà essere periodicamente aggiornata in base al livello di rischio ottenuto e, in ogni caso, sottoposta a riesame con cadenza almeno annuale, nonché ogni volta il trattamento dovesse subire delle modifiche.
Nell'effettuazione dell'Analisi del rischio, gli esercenti le funzioni di titolare del trattamento fanno riferimento alla metodologia allegata al presente atto (Allegato 4).

Art. 5
(Valutazione d'impatto)

Laddove un trattamento comporti un rischio elevato per i diritti e le libertà delle persone interessate, gli esercenti le funzioni di titolare del trattamento, in base a quanto prescritto dal DM 37 del 10 aprile 2019 e ss.mm.ii., procedono, ai sensi dell'art. 35 del Regolamento (UE) 2016/679, all'effettuazione della Valutazione d'Impatto.

La Valutazione d'Impatto contiene almeno:

1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. il contesto normativo di riferimento;
3. una descrizione del rispetto dei principi di protezione dei dati enunciati dalla normativa in materia di protezione dei dati personali, incluso, in particolare il Regolamento (UE) 679/2016 (esattezza, trasparenza, liceità, minimizzazione, esercizio dei diritti degli interessati, limitazione delle finalità, limitazione della conservazione dei dati);
4. una valutazione dei rischi per i diritti e le libertà degli Interessati;
5. le misure di sicurezza 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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

La Valutazione di Impatto sulla protezione dei dati deve essere condotta prima di procedere al trattamento, in fase di definizione dello stesso, e deve essere sottoposta a un continuo riesame, ripetendo la valutazione a intervalli regolari o, comunque, appena intervengono sostanziali modifiche al contesto del trattamento.

Laddove richiesto, il RPD fornisce un parere in merito alla valutazione d'impatto e ne sorveglia lo svolgimento ai sensi dell'art. 35 del GDPR.

Nell'effettuazione della Valutazione d'Impatto, gli esercenti le funzioni di titolare del trattamento fanno riferimento alla metodologia di Valutazione d'Impatto allegata al presente atto (Allegato 5).

Art. 6

(Informative)

Gli esercenti le funzioni di titolare del trattamento, in base a quanto prescritto dal DM 37 del 10 aprile 2019 e ss.mm.ii., provvedono a:

- definire o aggiornare le informative, che devono essere adeguate nella forma e nel linguaggio alla tipologia di soggetto interessato (per esempio: dipendenti, utenti, minori, ecc.) e devono contenere tutte le informazioni necessarie a comprendere l'identità e i dati di contatto del titolare e del RPD, la descrizione delle modalità e le finalità del trattamento, la base giuridica, etc.;
- garantire che le informative, una volta diffuse e condivise o siano sempre disponibili o, comunque, facilmente reperibili attraverso canali individuati (fisici e telematici) e che vengano aggiornate a valle dell'attività di valutazione e modifica del registro delle attività di trattamento.

L'informativa, in ossequio a quanto previsto dalla normativa vigente, deve essere fornita all'interessato in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in modo tale che l'interessato sia effettivamente messo a conoscenza circa le concrete modalità di trattamento dei propri dati personali.

Le informazioni contenute all'interno delle informative devono essere costantemente aggiornate dovendo queste fornire una rappresentazione fedele delle operazioni di trattamento svolte dal titolare del trattamento sui dati personali del soggetto interessato.

Gli esercenti le funzioni di titolare del trattamento nell'elaborazione delle informative da fornire agli interessati, fanno riferimento allo standard di informativa allegato al presente atto (Allegato 6).

Art. 7

(Gestione delle richieste degli interessati)

Il RPD funge da punto di contatto con gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti previsti dagli artt. 15-22 del GDPR e pertanto è il soggetto deputato a fornire riscontro all'interessato, al più tardi entro un mese dalla ricezione della richiesta (tale termine può essere prolungato fino ad un massimo di tre mesi, se necessario, tenuto conto della complessità e del numero delle richieste formulate dall'interessato).

Ciascun Ufficio del Ministero, al fine di consentire il riscontro alle istanze pervenute da parte degli interessati, su richiesta del RPD, fornisce le informazioni necessarie a gestire le istanze di esercizio dei diritti degli interessati nel rispetto dei principi previsti dal GDPR.

Nell'ambito delle già menzionate attività, il personale del Ministero fa riferimento a quanto prescritto all'interno della procedura per la gestione dei diritti dell'interessato adottata dal Ministero (Allegato 7).

Art. 8

(Violazioni di dati personali)

In caso di *data breach*, ossia in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati, è necessario mettere in atto le seguenti attività:

1. identificazione di un potenziale *data breach*. Tutte le possibili violazioni dei dati personali devono essere identificate e indirizzate tempestivamente al Responsabile della protezione dei dati. Quest'ultimo, una volta ricevuta la comunicazione sul potenziale *data breach*, individua il soggetto che esercita le funzioni di titolare che sarà competente per la gestione della eventuale violazione e trasmette senza ritardo la comunicazione ai referenti privacy della struttura individuata. Il referente privacy inoltra la comunicazione pervenuta al responsabile o ai responsabili interni e collabora con gli stessi nell'attività di valutazione del livello e delle potenzialità di rischio per gli interessati dell'evento descritto nella comunicazione;
2. esecuzione dei riscontri interni. Il responsabile interno del trattamento interessato, con l'ausilio dei referenti privacy, nonché avvalendosi della collaborazione degli autorizzati al trattamento e degli amministratori di sistema, ricevuta la comunicazione della presunta violazione di dati personali, effettua alcune verifiche interne volte a vagliarne l'attendibilità. In caso di riscontrata violazione di dati personali, il responsabile interno comunica al soggetto che esercita le funzioni di titolare e al RPD l'avvenuta violazione;
3. valutazione e mitigazione. Il soggetto che esercita le funzioni di titolare del trattamento, ricevuta la comunicazione della violazione, valuta la complessità della stessa. Per ciascuna violazione dei dati personali, devono essere identificate opportune misure correttive tecniche e organizzative da adottare, al fine di mitigare i relativi effetti e ridurre la probabilità di impatto e ricorrenza. Le misure di mitigazione dovranno essere adeguate alla natura della violazione dei dati personali;
4. notifica all'Autorità Garante. Qualora risulti probabile che il *data breach* possa rappresentare un rischio per i diritti e le libertà degli interessati, il soggetto che esercita le funzioni di titolare del trattamento è tenuto a notificare l'avvenuta violazione di dati personali all'Autorità Garante entro 72 ore;
5. comunicazione agli interessati. Qualora l'esito della valutazione rappresenti che la violazione dei dati personali è suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, il soggetto che esercita le funzioni di titolare del trattamento, con il supporto del RPD, predispone la comunicazione agli interessati e la trasmette al Segretario Generale. Quest'ultimo comunica la violazione all'interessato, o agli interessati, senza ingiustificato ritardo, utilizzando i canali ufficiali di comunicazione a disposizione del Ministero;
6. aggiornamento del registro delle violazioni. Il soggetto che esercita le funzioni di titolare del trattamento, con il supporto dei referenti privacy, una volta terminate le fasi precedenti, procede all'aggiornamento del registro delle violazioni;

7. definizione del piano di rimedio. Una volta concluso il processo di notifica e comunicazione della violazione di dati personali agli interessati, il soggetto che esercita le funzioni di titolare del trattamento, supportato dal RPD, definisce un piano di rimedio al fine di garantire un livello di sicurezza adeguato ai rischi in ordine alla protezione dei dati personali trattati.

Tali attività sono dettagliate all'interno della procedura relativa alla gestione delle violazioni di dati personali, in allegato alla presente Direttiva (Allegato 8).

Art. 9

(Formazione del personale)

Il Ministero, in linea con la propria articolazione interna e con l'attribuzione dei ruoli e delle responsabilità definita dal D.M. n. 37 del 10 aprile 2019 e ss.mm.ii., tramite il coordinamento del Responsabile della Protezione dei Dati, al fine di garantire la diffusione, all'interno dell'Amministrazione, di una cultura della privacy, e fornire gli strumenti adeguati per assicurare il rispetto della normativa in materia di dati personali, assicura la programmazione e l'organizzazione di campagne di formazione e iniziative specifiche sui temi principali e più rilevanti in materia di privacy e *data protection*.

Art. 10

(Attività di verifica e controllo dei trattamenti di dati personali)

Tutte le Strutture del Ministero supportano il RPD nelle attività di sorveglianza della corretta applicazione del Regolamento e di altre disposizioni dell'Unione Europea o nazionali, relative alla protezione dei dati personali, previste dall'articolo 39 paragrafo 1.b del Regolamento (UE) 2016/679, fornendo, quando richiesto, ogni evidenza necessaria all'espletamento di tale attività.

Le attività di sorveglianza comprendono, tra l'altro:

1. la verifica della completezza e della correttezza delle informazioni inserite nel registro dei trattamenti;
2. la verifica della corretta predisposizione e gestione delle attività inerenti e connesse al trattamento (gestione dell'informativa, gestione del consenso, gestione dei diritti dell'interessato, gestione del rischio, valutazione d'impatto, gestione dei *data breach*);
3. la verifica dell'applicazione e dell'efficacia delle misure di sicurezza adottate;
4. la verifica dell'applicazione delle istruzioni per la corretta gestione dei trattamenti.

In particolare, con riferimento all'attività di verifica per l'applicazione e l'efficacia delle misure di sicurezza di cui al punto 3, l'Amministrazione si è dotata di una apposita procedura "per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza dei trattamenti

di dati personali", all'interno della quale sono dettagliate tali attività (Allegato 9).

L'esercente le funzioni di titolare, ai sensi dell'articolo 3, comma 2, del DM n. 37 del 10 aprile 2019 e ss.mm.ii., redige una relazione semestrale in cui illustra al Responsabile della Protezione dei Dati tutte le iniziative intraprese e da intraprendere per quanto attiene alla protezione dei dati personali.

Art. 11

(Gestione dei documenti informatici e cartacei)

Ciascuna struttura del Ministero gestisce le informazioni nel rispetto delle leggi e dei regolamenti vigenti, in particolare nel rispetto dei principi a tutela della privacy, nonché di quelli di trasparenza, correttezza, responsabilità e sostenibilità.

Ciascuna risorsa del Ministero nell'esecuzione dei propri compiti e mansioni, al fine di proteggere il patrimonio informativo dei propri utenti, segue quanto prescritto all'interno della "Politica sulla Sicurezza delle informazioni", allegata al presente atto (Allegato 10).

Di seguito si riportano alcune prescrizioni fornite ai dipendenti (utenti) del Ministero e relative ad aspetti di interesse comune su tematiche specifiche:

Uso delle stampanti

L'utente, al fine di minimizzare il rischio di diffusione non autorizzata di informazioni, potrà procedere all'avvio della stampa esclusivamente attraverso il *badge* personale in uso. L'utente, dunque, invierà il documento in stampa e il dispositivo rilascerà i documenti solo quando il mittente avrà effettuato il *log-in* con il proprio *badge*.

Clean Desk Policy

Gli utenti sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti cartacei.
Gli utenti adottano una "politica della scrivania pulita" (*Clean Desk Policy*), ovvero si richiede di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali. È opportuno, inoltre, che gli archivi fisici di dati aziendali, in particolari gli archivi contenenti dati personali, di tipo "sensibili" e/o "giudiziari", ai sensi della normativa sulla privacy, siano conservati in contenitori dotati di chiave (armadi, cassettiere, schedari) e, nel caso di allontanamento temporaneo del lavoratore dalla propria postazione di lavoro, gli stessi non devono essere lasciati incustoditi.

Dispositivi informatici

L'Amministrazione è esclusiva titolare e proprietaria dei dispositivi informatici messi a disposizione degli utenti, nonché delle informazioni e dati personali in essi contenute e/o trattate; tali informazioni o dati devono essere trattati dagli utenti adottando criteri di adeguata riservatezza nella comunicazione dei dati

conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta. I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità degli utenti esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali.
Gli utenti nell'utilizzo dei dispositivi messi a disposizione dall'Amministrazione devono seguire delle specifiche regole di buon uso volte alla tutela dei dati personali ivi contenuti.

Posta Elettronica

L'utilizzo della posta elettronica è connesso allo svolgimento dell'attività lavorativa; pertanto, è da evitare l'utilizzo della posta elettronica per motivi personali.
Gli utenti hanno in utilizzo indirizzi nominativi di posta elettronica. Possono essere assegnate anche caselle e-mail con natura impersonale (ad esempio info, amministrazione, direzione); in questi casi, è preferibile evitare che il destinatario delle mail possa considerare l'indirizzo assegnato come "privato".
L'utilizzo della posta elettronica deve essere effettuato dall'utente con la massima diligenza.

Password

Al fine di elevare i requisiti di sicurezza nell'accesso alle risorse di rete del Ministero, la *password* dei pc dovrà essere composta da almeno 12 caratteri e rispettare specifici requisiti. Nel dettaglio, i requisiti minimi per la composizione della *password*:

- non potrà contenere parti significative del nome di account o del nome dell'utente;
- dovrà contenere caratteri appartenenti a tre delle quattro categorie seguenti:
  - lettere maiuscole;
  - lettere minuscole;
  - i primi 10 numeri di base;
  - caratteri speciali (ad esempio: !, $, #, %).

Di seguito si riportano dei consigli utili per creare e scegliere una *password* in sicurezza:

- non utilizzare la stessa password per più account (ad esempio per mail private o altri servizi internet);
- non utilizzare una password contenente dati personali, come ad esempio date e nomi - non solo di persone, ma anche di animali domestici – oppure il codice fiscale etc.;
- non usare parole o acronimi che si possono trovare nel dizionario o frasi famose;
- non usare sequenze di tasti sulla tastiera (asdf, qwerty) o sequenze di numeri (1234);
- non usare ripetizioni di caratteri (aa11).

La *password* individuata non dovrà essere comunicata a soggetti terzi e non dovrà essere conservata in luoghi facilmente accessibili. È, altresì, consigliato non usare la password su computer pubblici o su connessioni *wi-fi* non sicure.

Il Ministro del Lavoro e delle Politiche Sociali

La presente Direttiva, unitamente agli allegati, è pubblicata sul sito istituzionale del Ministero del lavoro e delle politiche sociali.

Roma, 11 GEN 2024

Marina Elvira Calderone

[redacted]