ISTITUTO NAZIONALE PER L'ANALISI DELLE POLITICHE PUBBLICHE

DETERMINA DEL DIRETTORE GENERALE

Oggetto: Adozione della procedura per i casi di violazione dei dati personali "Data Breach", in conformità agli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679)

VISTI:

il Decreto del Presidente della Repubblica 30 giugno 1973, n. 478 costitutivo dell'Istituto per lo Sviluppo della Formazione professionale dei Lavoratori (ISFOL) e s.m.i.;

il Decreto Legislativo 24 settembre 2016, n. 185 ed in particolare l'articolo 4, co. 1, lett. f), che a decorrere dal 1° dicembre 2016, modifica la denominazione dell'ISFOL in INAPP - Istituto Nazionale per l'Analisi delle Politiche Pubbliche, lasciando invariati tutti gli altri dati dell'Istituto;

il D.P.R. 27 febbraio 2003, n. 97 che regolamenta l'amministrazione e la contabilità degli Enti pubblici di cui alla Legge 20 marzo 1975, n. 70;

lo Statuto dell'INAPP, approvato con Delibera del Consiglio di Amministrazione 17 gennaio 2018, n. 2 ed in vigore dal 2 maggio 2018;

il vigente Regolamento di organizzazione e funzionamento degli Organi e delle Strutture dell'Istituto, come approvato con Delibera del Consiglio di Amministrazione del 18 dicembre 2020, n. 18;

il Decreto del Ministro del Lavoro e delle Politiche sociali 3 febbraio 2020, n. 22 con il quale il Prof. Sebastiano Fadda è stato nominato Presidente dell'INAPP;

la Delibera del Consiglio di Amministrazione 19 febbraio 2020, n. 1 di nomina del Dott. Santo Darko Grillo a Direttore Generale dell'INAPP;

il Decreto del Ministro del Lavoro e delle Politiche sociali n. 183 del 29 settembre 2021 con il quale è stato nominato il Consiglio di Amministrazione dell'INAPP;

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, di seguito "Regolamento");

il Decreto Legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal 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» (di seguito "Codice");

il Decreto Legislativo 18 maggio 2018, n. 51, recante 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 (di seguito "D.Lgs. n. 51/2018");

le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato Europeo per la protezione dei dati il 25 maggio 2018;

il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (*Data breach*) - 30 luglio 2019 [doc-web n. 9126951];

CONSIDERATO che, in caso di violazione dei dati personali, il titolare del trattamento

è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del Regolamento, art. 2-bis del Codice);

CONSIDERATO che l'Istituto Nazionale per l'Analisi delle Politiche Pubbliche – INAPP (di seguito anche "Istituto" o "Ente"), rappresentato dal suo Presidente, Prof. Sebastiano Fadda, è Titolare del trattamento dei dati personali ai sensi dell'art. 4, n. 7 del Regolamento e del D.Lgs. n. 196/2003 e s.m.i., con le responsabilità che discendono dalla citata normativa e dalle ulteriori norme, provvedimenti e linee guida integrative adottate dal legislatore nazionale, dall'Autorità Garante per la protezione dei dati personali e dall'European Data Protection Board (di seguito, unitariamente definiti anche come "Norme e Provvedimenti vigenti");

TENUTO CONTO che, con atto di delega di funzioni del 27 aprile 2020, ai sensi dell'art. 2-*quaterdecies* del D.Lgs. n. 196/2003 e s.m.i. (prot. n. 0000426), il Titolare del trattamento ha affidato al Direttore Generale, Dott. Santo Darko Grillo, la gestione operativa dei principali compiti e funzioni relative al trattamento dei dati personali dell'Istituto, conformemente agli standard imposti dal Regolamento UE 2016/679 (RGPD) e dalla normativa nazionale integrativa in materia ivi richiamata;

CONSIDERATO che il Titolare del trattamento è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (*Data Breach*), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

TENUTO CONTO che il Titolare del trattamento è tenuto, altresì, a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del Pubblico Ministero (artt. 26 e 37, comma 6, del D.Lgs. n. 51/2018);

CONSIDERATO che, per «violazione dei dati personali» (*Data Breach*), si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12, del Regolamento; art. 2, comma 1, lett. m, D.Lgs. n. 51/2018);

TENUTO CONTO che per la omessa notifica di *Data Breach* all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);

TENUTO CONTO, inoltre, che l'art. 82 GDPR prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del medesimo Regolamento ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile);

TENUTO CONTO che lo stesso GDPR, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può

sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del Titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta, inoltre, sicuramente un'attenuazione delle sanzioni applicabili;

PRESO ATTO della fondamentale importanza di adottare una procedura organizzativa interna destinata alla gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Istituto;

DETERMINA

1. le premesse e gli atti nelle stesse richiamati costituiscono parte integrante e sostanziale del presente provvedimento;

2. di adottare, in conformità agli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679), l'allegata Procedura per la gestione delle violazioni dei dati personali ("*Data Breach*"), comprensiva dei relativi allegati; M01 - Modulo Gestione Data Breach e M02 – Modulo Registro incidenti Data Breach. Tale procedura, comprensiva dei suddetti allegati, costituisce parte integrante e sostanziale del presente provvedimento;

3. di demandare la concreta attuazione delle misure regolamentari minime contenute nella Procedura di cui al precedente punto 2 al personale operante all'interno dell'INAPP nelle sue articolazioni gerarchiche e secondo le rispettive funzioni e competenze;

4. di dare atto che le disposizioni operative della Procedura di cui al precedente punto 2 sono soggette a revisione ogni qualvolta ciò si dovesse rendere necessario e, comunque, a cadenza almeno annuale;

5. di disporre che al presente provvedimento venga assicurata: a) pubblicità con pubblicazione sul sito istituzionale dell'Istituto, nonché b) la massima diffusione presso tutto il personale operante in Istituto e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento.

Il Direttore Generale

Dott. Santo Darko Grillo

Documento sottoscritto con firma digitale ai sensi del D.Lgs. n. 82/2005 e s.m.i.