PROCEDURA PER LA VALUTAZIONE DEI RISCHI E PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI ("*DPIA*")

INDICE DELLA PROCEDURA

***** *** *****

I. POLITICA

È politica dell'Azienda di Servizi alla Persona Istituti Milanesi Martinitt e Stelline e Pio Albergo Trivulzio ("Asp" o "Ente") proteggere la sicurezza e la riservatezza dei dati personali (soprattutto dei pazienti e del

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

personale), identificando le cause più probabili di rischio all'interno dell'Ente, valutare il grado di esposizione, determinare e realizzare le misure per la sicurezza e la riservatezza dei dati personali ai sensi e per gli effetti del Regolamento Europeo 679/2016 (da ora in poi anche "GDPR").

II. AMBITO DI APPLICAZIONE

La presente procedura si applica al trattamento dei dati personali effettuati dall'Ente.
Tutto il personale che opera nell'Ente è tenuto al rispetto della presente procedura.
In particolare, sono tenuti al rispetto della procedura i seguenti soggetti: il Titolare del trattamento, i Designati al trattamento, i Referenti al trattamento, gli Autorizzati al trattamento, il DPO, se soggetto interno (art. 8, comma tre, art. 24, comma 3, punto 3, art. 17, comma tre, punto c del Regolamento sulla protezione dei dati personali).
La tempestività della valutazione è un fattore determinante per il rispetto delle prescrizioni del GDPR.

III. SCOPO

Lo scopo di questa procedura è fornire uno strumento in grado di definire un processo per la gestione delle attività relative alla valutazione dei rischi inerenti i trattamenti dei dati personali effettuati dall'Ente e le linee guida per condurre una Valutazione di Impatto.
In particolare, lo scopo è:

- SEZIONE UNO - definire i processi/le attività da seguire per l'analisi del rischio privacy dei trattamenti dei dati;
- SEZIONE DUE - definire il processo/le fasi per la conduzione della Valutazione d'impatto sulla protezione dei dati" (c.d. *Data Protection Impact Assessment* – "DPIA"), così come prescritto dall'art. 35 del GDPR.

IV. TERMINI E DEFINIZIONI

Di seguito, si elencano alcune definizioni utili ai fini della presente procedura[1]:

- Trattamento = "*Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*" (art. 4, comma uno, n. 2 GDPR);
- Sicurezza del trattamento = "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*", (primo comma art. 32 GDPR);
- Rischio = scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà dell'interessato: il rischio si riferisce al soggetto interessato;
- Valutazione di impatto o "DPIA" = procedura prevista dall'art. 35 GDPR che mira a descrivere un trattamento di dati per valutare la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli.

[1] Per le altre definizioni in tema privacy si fa riferimento al Regolamento dell'Ente per la protezione dei dati personali.

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

SEZIONE UNO: VALUTAZIONE DEI RISCHI DEL TRATTAMENTO DEI DATI

1. Definizione dell'operazione di trattamento e del suo contesto

Prima di ogni valutazione del rischio, il Titolare del trattamento deve individuare le operazioni di trattamento dei dati. Le operazioni di trattamento dei dati devono essere registrate nel registro delle attività di trattamento predisposto e tenuto dall'Ente ai sensi dell'art. 30 GDPR.

2. Comprensione e valutazione dell'impatto

In questa fase, il Titolare del trattamento deve valutare l'impatto sui diritti e sulle libertà fondamentali delle persone fisiche derivanti dalla possibile perdita di sicurezza dei dati personali.
Devono essere considerati quattro livelli di impatto (Basso, Medio, Alto, Molto Alto):

- Basso = l'impatto è basso quando gli interessati andranno incontro a disagi minori che supereranno senza problemi (tempo trascorso reinserendo le informazioni, fastidi, irritazioni, etc.);
- Medio = l'impatto è medio quando gli interessati possono avere significativi disagi che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di acceso ai servizi aziendali, paura, stress, mancanza di comprensione, disturbi fisici di lieve entità, etc.);
- Alto = l'impatto è alto quando potranno esserci conseguenze significative che gli interessati dovrebbero riuscire a superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, perdita di posti di lavoro, danni alla proprietà, citazioni in giudizio, etc., peggioramento della salute);
- Molto alto = l'impatto è molto alto quando gli interessati potranno subire conseguenze significative o irreversibili che non saranno in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, etc.).

La valutazione è un processo qualitativo e il Titolare del trattamento deve considerare una serie di fattori quali la tipologia di dati personali, la criticità dell'operazione di trattamento, il volume dei dati personali (etc.).

Il Titolare del trattamento deve compilare l'allegato A (Modello per la pre-valutazione del rischio) nel software "UTOPIA", con il supporto dei Sistemi Informativi (anche con l'ausilio dell'allegato A.1.- Elenco Asset e Vulnerabilità).

3. Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia)

In questa fase lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno ed interno) e valutare la probabilità (probabilità di accadimento della minaccia).
Il Titolare del trattamento, deve compilare le tabelle relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati (da lettera B a lettera E dell'Allegato A - Modello per la Pre-valutazione del rischio): 1) risorse di rete e tecniche (hardware e software), 2) processi /procedure relativi all'operazione di trattamento dei dati, 3) diverse parti e persone coinvolte nell'operazione di trattamento, 4) settore di operatività e scala del trattamento nel software "UTOPIA".

4. Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto)

Con l'ausilio del software "UTOPIA", una volta inserite tutte le informazioni richieste dall'Allegato A, l'Ente otterrà la valutazione del rischio, calcolata secondo il metodo "ENISA".

5. Misure di sicurezza

A seguito della valutazione del livello di rischio, il Titolare del trattamento deve selezionare le misure di sicurezza appropriate per la protezione dei dati personali.
Le misure possono essere di due categorie: misure organizzative e misure tecniche.

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

SEZIONE DUE: VALUTAZIONE DI IMPATTO

1. DEFINIZIONE PRELIMINARE DI DPIA

La DPIA è una procedura volta ad analizzare il processo di trattamento, al fine di determinare se quest'ultimo presenti rischi per i diritti e le libertà delle persone associati a un trattamento di dati e, quindi, sia necessario adottare misure tecniche e organizzative ulteriori a quelle programmate per mitigare tali rischi, prescritta dall'art. 35 GDPR.

Quando si parla di "rischi per i diritti e le libertà delle persone" ci si riferisce a qualunque effetto che il trattamento potrebbe avere sui diritti e sulle libertà fondamentali delle persone: libertà di espressione, libertà di pensiero, diritto a non subire discriminazioni, libertà di coscienza, libertà religiosa.

Nell'identificare i rischi si deve considerare qualsiasi impatto che il trattamento potrebbe avere sulle persone (fisico, economico, emotivo).
I potenziali impatti comprendono, ad esempio:

- impossibilità di accedere a servizi o ad altre opportunità,
- discriminazione,
- furto di identità e altre frodi,
- perdite economiche,
- danni alla reputazione,
- danni fisici,
- compromissione della confidenzialità,
- impossibilità di esercitare eventuali diritti.

Gli impatti possono concretizzarsi per due motivi principali:

1. il trattamento, per come è stato progettato, potrebbe provocare tali impatti (per es. a causa del tipo di dati trattati, a causa delle persone che vi hanno accesso, a causa del possibile effetto del trattamento, etc.);
2. la sicurezza dei dati, in termini di compromissione della confidenzialità, dell'integrità o della disponibilità dei dati.

1.2. QUANDO SI DEVE PROCEDERE ALLA DPIA?

La valutazione di impatto sulla protezione dei dati va effettuata prima del trattamento: va avviata, il prima possibile, nella fase di progettazione del trattamento.
Il Titolare del trattamento deve valutare la necessità di effettuare una DPIA quando:

(I) si intende:
   a. procedere all'acquisto di un bene (per esempio, software, hardware, apparati di rete, etc.) o di un servizio,
   b. progettare o implementare un nuovo processo o
   c. procedere alla modifica dei processi già in corso (intesa come modifica del flusso operativo o degli strumenti utilizzati per il trattamento come nel caso dell'acquisto o comunque dell'utilizzo di nuovi software, hardware, reti, piattaforme, etc.) o

(II) intervengano modifiche del contesto in cui si svolgono in caso di utilizzo di nuove tecnologie.

Il Titolare del trattamento deve consultare il DPO e il parere ricevuto dal DPO deve essere documentato all'interno della relazione della DPIA (art. 35, comma 2, GDPR).
Il Titolare del trattamento, se del caso, raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto (art. 35, comma 9, GDPR).

Sono individuate le seguenti fasi per effettuare la DPIA:

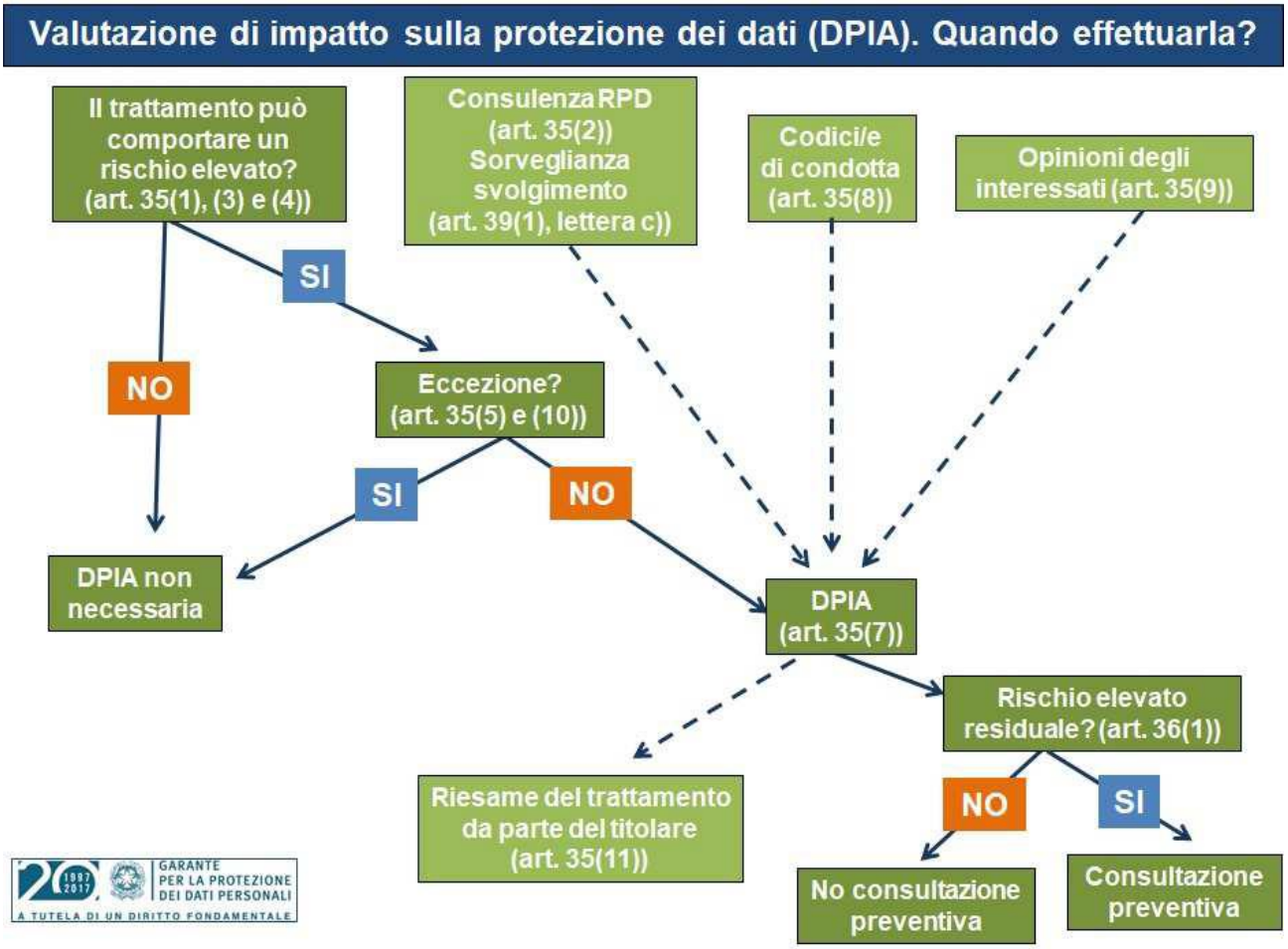
- valutazione della necessità di condurre una attività di DPIA,
- valutazione della conformità del trattamento al GDPR,
- descrizione del trattamento,
- valutazione dei rischi,

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

- analisi del rischio,
- piano di azione,
- monitoraggio del trattamento.

Il Titolare del trattamento deve compilare gli allegati (di seguito specificati, da B a F) prodromici alla implementazione del software "UTOPIA" della sezione "IMPATTO": gli allegati dovranno poi essere allegati nel software "UTOPIA".

1.3. SCHEMA



2. VALUTAZIONE DELLA NECESSITA' DI CONDURRE UN'ATTIVITA' DI DPIA

Questa fase ha l'obiettivo di stabilire se rispetto ad una determinata attività ricorra o meno la necessità di effettuare una DPIA.

Si tratta di una prima analisi preliminare.

Due sono gli strumenti necessari da consultare e da utilizzare per questa fase di valutazione.

Prima si valuta se il trattamento rientra in una delle categorie come da elenco dell'Autorità Garante per la Protezione dei Dati Personali (All. 1 – Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto - allegato 1 al provvedimento n. 467 dell'11 ottobre 2018.

Dopo si valuta se il trattamento presenta almeno due dei criteri stabiliti dal WP 248 rev. 01 (All. 2 – Info grafica predisposta dall'Autorità Garante per la Protezione dei Dati Personali), di seguito elencati:

- trattamenti valutati o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es. videosorveglianza);

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es. informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insieme di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, decive IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

QUANDO È POSSIBILE NON EFFETTUARE UNA DPIA

Una valutazione di impatto sulla protezione dei dati, non è richiesta nei seguenti casi di trattamento:

- quando il trattamento non "*presenta un rischio elevato per i diritti e le libertà delle persone fisiche*";
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati;
- è già stato sottoposto a verifica da parte di un'Autorità di controllo prima del maggio 2019 e le cui condizioni (es. oggetto, finalità, ecc.) non hanno subito modifiche;
- è ricompreso nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fa riferimento a norme e regolamenti, UE o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Ove il Titolare del trattamento dovesse valutare che il trattamento non presenti un rischio elevato e, quindi, che non si necessario effettuare una DPIA, il Titolare del trattamento dovrà motivare e documentare l'analisi effettuata e la predetta relazione dovrà essere conservata in atti.

3. DESCRIZIONE DEL TRATTAMENTO

La descrizione del trattamento e del contesto in cui si svolge è fondamentale per determinare i potenziali rischi che il trattamento comporta.
Si tratta di descrivere il ciclo di vita dell'informazione, ad esempio, in termini di raccolta, archiviazione, utilizzo e cancellazione: la descrizione dei flussi dei dati è fondamentale perché solo una precisa comprensione dell'impiego dei dati trattati consente di evidenziare i rischi del trattamento.
La descrizione ha, quindi, lo scopo di evidenziare: quale informazione viene usata, le finalità del trattamento, le modalità, i soggetti che accedono alle informazioni, gli strumenti utilizzati per il trattamento stesso.
È necessario rispondere alle seguenti domande dell'Allegato B (*Check list* per la descrizione del trattamento).

4. VALUTAZIONE DELLA CONFORMITA' DEL TRATTAMENTO AL GDPR

In questa fase si procede ad un'analisi della liceità, della necessità e della proporzionalità del trattamento rispetto alle finalità, con lo scopo di rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate e gli interessi legittimi del Titolare del trattamento.
Le misure previste per conformarsi al GDPR, sono valutate attraverso la valutazione delle seguenti sezioni di interessi:

1. misure che contribuiscono alla proporzionalità e necessità del trattamento,
2. misure che contribuiscono ai diritti delle persone interessate,
3. liceità.

Per ogni categoria (1, 2, 3) si dovrà tener conto delle *check list* allegate (sub allegato B): le risposte date alle singole domande sono parte integrante e sostanziale della relazione della DPIA.

5. VALUTAZIONE DEI RISCHI

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

In questa fase vanno identificati quali potenziali minacce possono riguardare gli interessati.
Le minacce sono legate a: contesto, strumenti e comportamento umano.
L'analisi dei rischi richiede la corretta identificazione delle minacce che possono aver successo sui dati coinvolti nel trattamento.
La valutazione dei rischi stabilisce il valore delle attività di informazione, identifica le minacce applicabili e le vulnerabilità che esistono (o possono esistere), identifica i controlli esistenti e il loro effetto sul rischio identificato, determina le potenziali conseguenze.
Le minacce che possono insidiare le tre caratteristiche fondamentali dei dati personali sono: riservatezza (R), integrità (I), disponibilità (D).

DEFINIZIONE	TIPOLOGIA DI VIOLAZIONE	EFFETTI
RISERVATEZZA	Accesso illegittimo	Divulgazione / Accesso non autorizzato
INTEGRITA'	Modifica indesiderata	Modifica
DISPONIBILITA'	Comparsa dei dati (compresa l'indisponibilità momentanea dei dati)	Distruzione / Perdita

Per la valutazione dei rischi, si dovrà compilare l'allegato C: le risposte date alla *Check list* "Analisi del Rischio" fanno parte integrante e sostanziale della relazione della DPIA.

6. ANALISI DEL RISCHIO

In questa fase è necessario valutare il rischio, considerando che uno o più eventi di natura dolosa o accidentale possono sfruttare le debolezze intrinseche del trattamento, causando un danno ai diritti e alle libertà degli interessati, con una certa probabilità di accadimento. Il livello di rischio è dato dal prodotto della probabilità di una minaccia per l'impatto della stessa.
Una volta valutato il trattamento (descrizione del trattamento, descrizione del rischio, fonte del rischio, impatti potenziali, minacce, etc.) si procede alla valutazione del rischio, con la collaborazione dei Sistemi Informativi (che potranno utilizzare l'allegato A.1 – Elenco Asset e Vulnerabilità).
Per la valutazione del rischio si utilizza il metodo "4X4": il rischio è = P x D (probabilità per gravità del danno); alla probabilità e alla gravità si assegna un numero compreso da 1 a 4.
Per la probabilità, i valori corrispondo alla seguente descrizione:
1 = Molto poco probabile (il suo verificarsi richiederebbe la concomitanza di più eventi poco probabili, non si sono mai verificati fatti analoghi, il suo verificarsi susciterebbe incredulità);
2 = Poco probabile (il suo verificarsi richiederebbe circostanze non comuni e di poca probabilità, si sono verificati pochi fatti analoghi, il suo verificarsi susciterebbe modesta sorpresa);
3 = Probabile (si sono verificati altri fatti analoghi, il suo verificarsi susciterebbe modesta sorpresa);
4 = Molto probabile (si sono verificati altri fatti analoghi, il suo verificarsi è praticamente dato per scontato).
Per la gravità, i valori di gravità sono i seguenti:
1 = Lieve
2 = Media
3 = Grave
4 = Molto grave
Una volta valutata la probabilità per la gravità del danno, si ottengono dei valori che si posso così sintetizzare nei seguenti valori di rischio.
R >= 9 (Elevato)
4 <= R <= 8 (Medio)
2 <= R <= 3 (Basso)
R = 1 (Minimo).
Il Titolare del trattamento, anche per l'analisi del rischio, utilizza il software "UTOPIA".

7. IL PIANO DI AZIONE

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

Il piano di azione consente di definire un piano condiviso delle misure da adottare, delle responsabilità di esecuzione e di verifica, di assunzione da parte del Titolare del trattamento, della consapevolezza del rischio residuo.
Con il piano di azione si rilevano le misure idonee da adottare, delle responsabilità di esecuzione e di verifica, di assunzione da parte del Titolare del trattamento della consapevolezza del rischio residuo.
I controlli che il Titolare del trattamento deve valutare per mitigare i rischi possono riguardare:

A. misure e controlli di tipo organizzativo, di: (i) Organizzazione e *governance*, (ii) Processi: procedure e policy interne, (iii) Formazione e consapevolezza;
B. misure e controlli di tipo tecnologico, quali, ad esempio: (i) anonimizzazione, (ii) pseudonimizzazione, (iii) cifratura dei dati, dei messaggi o degli archivi;
C. misure e controlli sui dati e sugli archivi.

Per il piano di azione, il Titolare del trattamento dovrà compilare l'allegato E: le risposte date alla *check list* "Il Piano di azione" (individuazione delle misure e riduzione del rischio) fanno parte integrante e sostanziale della relazione della DPIA.
Se il rischio rimane alto, il Titolare del trattamento, ai sensi dell'art. 36 GDPR, dovrà procedere alla comunicazione all'Autorità Garante per la Protezione dei Dati Personali.

8. MONITORAGGIO DEL TRATTAMENTO

La DPIA è un processo continuo che deve essere costantemente oggetto di integrazione e aggiornamento:

- ove vengano acquisite ulteriori informazioni ovvero,
- intervengono modifiche negli strumenti utilizzati per il trattamento dei dati ovvero,
- siano apportati cambiamenti significativi al trattamento ovvero,
- in occasione di ogni cambiamento del livello di rischio (art. 35, comma 11, GDPR) ovvero,
- intervengono cambiamenti nei processi (contesto organizzativo o nel contesto sociale) in cui si svolgono i trattamenti.

Il Trattamento deve essere costantemente monitorato per individuare tempestivamente i rischi privacy.
Il monitoraggio è, dunque, volto a rilevare eventuali cambiamenti dei rischi (derivanti da modifiche del trattamento o da mutamenti della percezione sociale del rischio).
Tali cambiamenti potrebbero richiedere una revisione della DPIA o persino una realizzazione *ex novo* della DPIA.

V. REGOLE GENERALI

Le varie fasi e i risultati della DPIA dovranno essere descritti in una relazione che dovrà documentare anche i pareri espressi dal DPO e la decisione finale assunta dal Titolare del trattamento in merito alla DPIA (approvazione DPIA, abbandono del progetto, decisione di consultare l'Autorità Garante per la Protezione dei Dati Personali ai sensi dell'art. 36 del GDPR).
La relazione potrà essere redatta utilizzando lo schema allegato (sub All. F) che fa propri gli altri allegati (sopra richiamati): relazione e allegati dovranno essere allegati nella sezione dedicata nel software "UTOPIA".
L'Ente utilizza, quindi, il software "UTOPIA" quale registro delle DPIA (dematerializzato): tale registro, inteso quale cartella nella quale, in un'ottica di *accountability*, vengono salvate tutte le DPIA dell'Ente e i report che documentano la scelta di non condurre una DPIA.

VI. VIOLAZIONE DELLA PRESENTE PROCEDURA

La violazione di quanto previsto nella presente Procedura espone il Titolare del Trattamento al rischio di responsabilità civile, penale e a sanzioni amministrative.
Tutto il personale è tenuto a prestare la massima collaborazione al Titolare del Trattamento; la mancata collaborazione in violazione delle norme del Codice Etico e di Comportamento dell'Ente potrà essere oggetto di provvedimento disciplinare.
Il soggetto autore delle violazioni potrà incorrere in responsabilità disciplinare e conseguentemente nei provvedimenti sanzionatori, secondo quanto previsto dalla normativa vigente.

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966

VII. RIFERIMENTI NORMATIVI E REGOLE INTERNE DELL'ASP

- Regolamento Europeo 679/2016
- Codice Privacy
- Manuale sulla Sicurezza nel trattamento dei dati personali di Enisa ("*European Union Agency for Network and Information Security*")
- Linee Guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato Europeo per la protezione dei dati il 25 maggio 2018 ("WP 248, rev. 01")
- Autorità Garante per la Protezione dei Dati Personali
- Regolamento sulla protezione dei dati personali adottato dall'Ente
- Procedura "Gestione delle violazioni di sicurezza dei dati"

VIII. ELENCO DEI DESTINATARI

- Tutto il personale dell'Ente
- DPO

IX. SCHEDE DI APPROFONDIMENTO

1. All. 1 – Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto (allegato 1 al provvedimento n. 467 dell'11 ottobre 2018);
2. All. 2 – Info-grafica Autorità Garante per la Protezione dei dati personali sulla Valutazione di Impatto sulla protezione dei dati (DPIA).

X. ALLEGATI

A. - Modello per la pre valutazione del rischio
A.1 - Elenco Asset e Vulnerabilità
B. *Check list* per la descrizione del trattamento e contesto di riferimento
C. *Check list* per la fase di valutazione della conformità del trattamento al GDPR
D. *Check list* di analisi del rischio
E. *Check list* per il piano di azione
F. Schema di valutazione di impatto (DPIA) – informazioni e allegati

ASP IMMeS e PAT
Via Marostica 8, 20146 Milano Tel. 02.4029.1
E-mail *ufficio.protocollo@pioalbergotrivulzio.it*
PEC *ufficio.protocollo@pioalbergotrivulzio.legalmail.it*
Codice Fiscale/Partita IVA: 04137830966