==========

FONDAZIONE "OPERA PIA ARPILI"
RESIDENZA PROTETTA - CASA DI RIPOSO
V I A L E D I A Z, N. 4 9

63846 M O N T E G I B E R T O

==========

DELIBERAZIONE N. 41 DEL 18.10.2025

OGGETTO: APPROVAZIONE PIANO DI PROTEZIONE DEI DATI PERSONALI E DI GESTIONE DEL RISCHIO DI VIOLAZIONE, NELL'AMBITO DELLE MISURE FINALIZZATE A DARE ATTUAZIONE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) N. 679/2016

==========

L'anno duemilaventicinque addì diciotto del mese di ottobre alle ore 17,00, in video conferenza.

Il Consiglio d'Amministrazione, riunitosi con l'intervento dei Sigg.:

COGNOME	NOME	QUALIFICA	PRESENTE	ASSENTE
ISOLINI	MARGHERITA	PRESIDENTE	X	
CATALINI	LEONELLA	COMPONENTE	X	
PIERGALLINA	ALESSANDRA	COMPONENTE	X	
RECCHI	LUIGINO	COMPONENTE	X	
SANTARELLI	ADORIANO	COMPONENTE	X	

assistito dal Segretario Amministrativo Dr. Fabrizio Annibali ha adottato la seguente deliberazione.

DELIBERA DEL CONSIGLIO D'AMMINISTRAZIONE N. 41 DEL 18.10.2025

OGGETTO: APPROVAZIONE AGGIORNAMENTO PIANO DI PROTEZIONE DEI DATI PERSONALI E DI GESTIONE DEL RISCHIO DI VIOLAZIONE, NELL'AMBITO DELLE MISURE FINALIZZATE A DARE ATTUAZIONE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) N. 679/2016

****

IL CONSIGLIO D'AMMINISTRAZIONE

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale é un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabilisce che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

CONSIDERATO che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:
–la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
–la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
–la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

TENUTO presente che tale evoluzione ha indotto l'Unione europea ad adottare 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 solo "GDPR");

DATO ATTO che il 24,05.2016 è entrato ufficialmente in vigore il GDPR, il quale diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25.05.2018;

RILEVATO che, con il GDPR, è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

RICHIAMATA la Legge 25.10.2017, n. 163 e, in particolare, l'art. 13, che ha delegato il Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

RILEVATO che il decreto legislativo delegato è finalizzato a realizzare l'adeguamento sulla base dei seguenti principi e criteri direttivi specifici:
a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al D.L.vo 30.06.2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
b) modificare il codice di cui al D.L.vo 30.06.2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;
d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;
e) adeguare, nell'ambito delle modifiche al codice di cui al D.L.vo 30.06.2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse;

RITENUTO che l'adeguamento dell'ordinamento nazionale interno al GDPR rende necessario definire le politiche e gli obiettivi strategici da conseguire per garantire l'adeguamento;

DATO ATTO che, sulla base del delineato quadro normativo, l'obiettivo di fondo del GDPR è la sicurezza del trattamento dei dati personali, programmando e pianificando gli interventi affinché i dati personali siano:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatto salvo l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

RITENUTO che l'obiettivo di assicurare la sicurezza dei dati richiede di gestire efficacemente, e conformemente alle disposizioni del GDPR, il rischio di violazione dei dati derivante dal trattamento, per tale dovendosi intendere 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 e che, a tal fine, vadano definiti gli obiettivi correlati alla gestione del rischio;

RITENUTO, pertanto, necessario procedere alla approvazione di un piano di protezione dei dati personali e di gestione del rischio di violazione, testo aggiornato rispetto a quello che era stato approvato con deliberazione consiliare n. 92 del 19.12.2024;

VISTO l'allegato schema di Piano di protezione dei dati e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016 di questa Fondazione per il triennio 2025/2027

APPURATO che:
- lo schema di piano copre il periodo del triennio 2025-2027;

- la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale;
- il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre più incisivi;
- l'adozione del documento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione;
- eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD;

CONSIDERATO che lo schema di Piano è stato predisposto dal responsabile del procedimento con il coinvolgimento e la partecipazione degli attori indicati nello Schema di Piano medesimo e, in particolare con la partecipazione dei responsabili di P.O. e il coinvolgimento del responsabile dei sistemi informativi;

RILEVATO che il Responsabile del procedimento è il Funzionario Amministrativo e Contabile Sig.ra Maria Paola Romanelli;

DATO ATTO che il Responsabile del procedimento, al fine di garantire il livello essenziale delle prestazioni, è tenuto a garantire la pubblicazione del presente provvedimento e dello schema di piano allegato sul sito web della Fondazione;

ACCERTATO che il RPD con nota in data 15.10.205 ha espresso il proprio parere favorevole al Piano di protezione dei dati e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016, di questa Fondazione per il triennio 2025/2027;

Con votazione palese unanime;

D E L I B E R A

1. Di approvare l'allegato aggiornato schema del Piano di protezione dei dati personali e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016, per il triennio 2025/2027 della Fondazione "Opera Pia Arpili" di Monte Giberto;

2. Di dare atto che il Piano copre il periodo di un triennio, 2025-2027 ed è soggetto ad aggiornamento annuale, e ad aggiornamenti anche infrannuali correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD;

3. Di comunicare i contenuti del Piano a tutti i dipendenti;

4. Di disporre che al presente provvedimento venga assicurata la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione;

5. Di dare atto che, in disparte le pubblicazioni sopra indicate, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.L.vo 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.L.vo 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.

6. Di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.L.vo 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

Letto, approvato e sottoscritto

IL PRESIDENTE
MARGHERITA ISOLINI

IL SEGRETARIO
DR. FABRIZIO ANNIBALI

FONDAZIONE "OPERA PIA ARPILI"

MONTE GIBERTO

PIANO 2025/2027 DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE[1]

per una gestione del rischio robusta

approvato con deliberazione del Consiglio di Amministrazione n. 41 del 18.10.2025 in adeguamento della norma UNI ISO 31000 e conforme al REGOLAMENTO UE 2016/679

[1] Il paragrafo 5.5.3 della norma UNI ISO 31000 prevede la predisposizione e l'adeguamento di "PIANI DI TRATTAMENTO DEL RISCHIO" aventi lo scopo di documentare come le opzioni di trattamento scelte sono attuate e indica, altresi', le informazioni da fornire nei suddetti piani.

TITOLO DEL DOCUMENTO: PIANO DI PROTEZIONE DEI DATI

Numero di versione: 03
Data ultimo aggiornamento: 06.10.2025
Stato del documento: Approvato dal Titolare con proprio provvedimento.
Estensori del documento: Titolare del trattamento
Riferimento per comunicazioni in merito al documento: Fondazione "Opera Pia Arpili" - Viale Diaz 49 - Telefono: 0734/630046 - email: info@arpili.it - Pec: arpili@pcert.postecert.it.
Modalità di distribuzione del presente documento e delle eventuali nuove versioni: Pubblicazione sul sito istituzionale, nella sezione Privacy.

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L"articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell"Unione europea ('Carta') e l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea ('TFUE') stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

Senonchè, la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali.

In adeguamento al GDPR (reg. UE 2016/679), il presente Piano di protezione dei dati personali (PPD) intende rappresentare lo strumento, il fulcro del sistema di protezione adottato dall'Ente.

PARTE I

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE (PPD)

DEFINIZIONI

Il presente documento recepisce e utilizza le seguenti definizioni:

- GDPR: il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR generale sulla protezione dei dati);
- 'WP29': gruppo di lavoro articolo 29 sulla protezione dei dati, per tale dovendosi intendere il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE quale organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata con i suoi compiti fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE;
- 'PPD': il presente Piano di Protèzione dei Dati personali e gestione del rischio di violazione;
- 'Regolamento dati sensibili': il Regolamento interno, approvato dal titolare in conformità allo schema tipo approvato dal Garante, che identifica e rende pubblici, per i trattamenti dei dati sensibili e giudiziari, i tipi di dati e le operazioni eseguibili;
- 'ID': identificativo.

OGGETTO

Il PPD individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle MISURE DI SICUREZZA informatiche/logiche, logistiche/fisiche, organizzative e procedurali da adottare e da applicare per ridurre/eliminare il RISCHIO di violazione dei dati derivante dal trattamento.

La disciplina si applica ai:

1.trattamenti con strumenti elettronici;

2.trattamenti senza l'ausilio di strumenti elettronici (ad esempio: cartacei, audio, visivi e audiovisivi, ecc.).

FINALITA'

Il presente documento, in attuazione del GDPR e della normativa interna di adeguamento, è funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali trattati nell'esercizio dell'attivita' istituzionale in un quadro di garanzie per gli interessati che contempla nuovi diritti.

Sul presupposto che costituisce un OBIETTIVO STRATEGICO la sicurezza del trattamento dei dati personali, scopo del presente documento è programmare e pianificare gli interventi affinchè i dati personali siano trattati conformemente ai principi dell'art. 5 del GDPR.

QUADRO NORMATIVO DI RIFERIMENTO

Il PPD tiene conto dei seguenti documenti:

- Codice in materia di dati personali (D.L.vo n.196/2003);
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- D.L.vo n. 101/2018 di adeguamento della normativa interna al GDPR;
- Dichiarazioni e Linee Guida del gruppo di lavoro articolo 29;
- Regolamenti interni, approvati dai titolari e/o dai responsabili.

DATA E PROVVEDIMENTO DI APPROVAZIONE

L'organo competente dell'intestato titolare ha approvato il PPD con provvedimento del Consiglio di Amministrazione nr. 41 del 18.10.2025.

PERIODO DI RIFERIMENTO E MODALITA' DI AGGIORNAMENTO

Il PPD copre il periodo del triennio 2025-2027, e la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale.

ATTORI INTERNI ALL'AMMINISTRAZIONE CHE HANNO PARTECIPATO ALLA PREDISPOSIZIONE DEL PIANO, NONCHE' CANALI E STRUMENTI DI PARTECIPAZIONE

Oltre al titolare, hanno contribuito alla predisposizione del Piano, per quanto di propria competenza:

- responsabili E.Q. delegati al trattamento e, loro tramite, gli incaricati del trattamento in relazione,
- responsabile della sicurezza dei sistemi informativi e responsabile IT;
- responsabile Protezione dei dati - RPD.

CANALI, STRUMENTI E INIZIATIVE DI COMUNICAZIONE DEI CONTENUTI

Il Piano viene portato alla conoscenza dei dipendenti, dei collaboratori, della cittadinanza e dei soggetti a qualunque titolo coinvolti nell'attivita' dell'ente mediante i seguenti strumenti:

- pubblicazione sul sito istituzionale a tempo indeterminato sino a revoca o sostituzione con un PPD aggiornato;
- invio a tutto il personale dipendente tramite rete intranet.

PARTE II

DATI PERSONALI, RISCHIO DI VIOLAZIONE E DISCIPLINA DEL GDPR

IL RISCHIO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E LA NEUTRALIZZAZIONE DEL RISCHIO ATTRAVERSO IL SISTEMA DI PROTEZIONE BASATO SU UNI ISO 31000

Nell'attuale contesto, lo sviluppo e la rapidità dell'evoluzione tecnologica nonchè la globalizzazione comportano nuove sfide per la protezione dei dati personali. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano.

Nel contempo, la tecnologia attuale consente a soggetti pubblici e privati di utilizzare dati personali come mai in precedenza, e la portata della condivisione e della raccolta di dati personali è' aumentata in modo significativo.

Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati, tenuto conto dell'aumento del rischio di violazione dei dati medesimi e della necessità che le persone fisiche abbiano il controllo dei dati personali che li riguardano in un quadro di certezza giuridica e operativa rafforzata così come delineata del GDPR.

Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e sui diritti degli interessati.
Rispetto a tali possibili impatti negativi, il titolare del trattamento è tenuto a promuovere e adottare approcci e politiche che tengano conto costantemente del rischio, effettuando una analisi attraverso un apposito processo di valutazione (si vedano artt. 35-36 GDPR) che sappia tenere conto:
- dei rischi noti o evidenziabili;
- delle misure tecniche e organizzative adottate o che si intende adottare per mitigare il rischio.
All'esito dell'analisi, condotta anche attraverso la valutazione di impatto (DPIA), il titolare del trattamento decide, in autonomia, se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale, fermo restando che l'autorità non ha il compito di "autorizzare" il trattamento, bensi' di indicare le misure ulteriori eventualmente da implementare a cura del titolare e puo', ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 GDPR (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

LA DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE
Le diverse componenti del sistema di protezione sono documentati almeno da:
- Piano protezione dati -PPD;
- Registri delle attività e delle categorie dei trattamenti;
- Mappa struttura organizzativa;
- Mappa dei soggetti;
- Mappa dei luoghi;
- Schede di ricognizione dei trattamenti/Indice-Mappa dei trattamenti;
- Mappa hardware;
- Mappa software;
- Mappa rischi e motivazioni stima;
- Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679/ Schede di assoggettabilità a DPIA;
- Schede di valutazione di impatto (DPIA) per i trattamenti a rischio elevato;
- Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente;
- Mappa delle misure di sicurezza logistiche/fisiche;
- Mappa delle misure di sicurezza informatiche/logiche;
- Mappa delle misure di sicurezza organizzative;
- Mappa delle misure di sicurezza e procedurali;
- Elenco delle misure di sicurezza correlate all'indice dei trattamenti e suddivise per uffici.

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000
Principi applicabili alla gestione del rischio
Sulla base della Norma UNI ISO 31.000, e ai fini della strategia di protezione dei dati personali, viene definita:
- la nozione di "rischio" come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.
- la nozione di "gestione dei rischi" come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta tenendo presente i principi contenuti nella Norma UNI ISO 31.000.
La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta attraverso le fasi di:
- analisi del rischio, quale fase del processo di gestione nella quale viene definito il contesto esterno e interno, di natura organizzativa e gestionale;
- valutazione del rischio, quale fase del processo di gestione del rischio che identifica, analizza e pondera il rischio medesimo;

- trattamento del rischio.

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA ANALISI
CONTESTO INTERNO ORGANIZZATIVO

L'articolo 35 del GDPR fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche".
Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.
I documenti allegati e, in particolare, la ricognizione dei trattamenti in rapporto a tutta l'attività dell'ente, le schede di DPIA e l'elenco dei rischi, della gravità rilevata dalla prospettiva degli interessati e della relativa motivazione comprovano l'effettuazione della analisi dei rischi derivanti dai trattamenti, e l'accuratezza della analisi medesima.

CONTESTO INTERNO ORGANIZZATIVO
STRUTTURA ORGANIZZATIVA

La struttura organizzativa dell'Ente è indicata nella MAPPA DELLA STRUTTURA ORGANIZZATIVA allegata, e corrisponde alle funzioni istituzionali e ai compiti assegnati a ciascuna struttura.
La MAPPA DEI LUOGHI indica:
- la sede principale, con l'indicazione degli Uffici e la relativa descrizione;
- le sedi secondarie, con l'indicazione degli Uffici e la relativa descrizione.

SOGGETTI: TITOLARE DEL TRATTAMENTO

Denominazione: Fondazione Opera Pia Arpili
Sede: Viale Diaz, nr. 49
Punti di contatto: arpili@libero.it - arpili@pcert.postecert.it
Il titolare del trattamento, sopra citato, esercita le funzioni e i compiti e assume le responsabilita' indicate nel GDPR e della normativa interna di recepimento.

SOGGETTI: CONTITOLARI DEL TRATTAMENTO

La MAPPA DEI SOGGETTI, allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i casi in cui il titolare, sopra indicato, e uno o più altri titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.
I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente GDPR, con particolare riguardo:
- all'esercizio dei diritti dell'interessato;
- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilita' siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.
Tale accordo deve designare un punto di contatto per gli interessati.

SOGGETTI: RESPONSABILI DEL TRATTAMENTO E SUB-RESPONSABILI

La MAPPA dei soggetti, allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i casi in cui un trattamento debba essere effettuato per conto del titolare del trattamento, da un responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.
Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.
Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri

responsabili del trattamento, dando cosi' al titolare del trattamento l'opportunità di opporsi a tali modifiche.

SOGGETTI: INCARICATI
La MAPPA dei soggetti, allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, l'Elenco dei casi in cui un il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali può trattare tali dati previa istruzione.

CONTESTO INTERNO GESTIONALE E OPERATIVO GDPR PER IL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI
L'Ente ha adottato, in adeguamento del D.L.vo 30.06.2003, n. 196, il GDPR per il trattamento dei dati sensibili e giudiziari che, identifica i tipi di dati sensibili e giudiziari e le operazioni eseguibili nello svolgimento delle proprie funzioni istituzionali con definizione dell'Indice dei trattamenti.

SCHEDE DI RICOGNIZIONE DEI TRATTAMENTI
Fanno parte del sistema di protezione le Schede di ricognizione dei trattamenti elaborate con riferimento a tutta l'attività svolta dall'Ente, prendendo in considerazione tutti i processi, inclusi i procedimenti amministrativi.

MAPPA HARDWARE
La Mappa hardware, allegata al presente documento per formarne parte integrante e sostanziale, identifica gli strumenti, i tipi di supporto e i locali di ubicazione. Fornisce, altresì, una descrizione delle caratteristiche tecniche degli strumenti elettronici medesimi.

MAPPA SOFTWARE
La Mappa software, allegata al presente documento per formarne parte integrante e sostanziale, identifica i software in relazione agli archivi/banche dati che vengono gestiti dai software medesimi. Identifica, altresi', i soggetti abilitati all'accesso.

MAPPA DEI RISCHI
La Mappa dei rischi, allegata al presente documento per formarne parte integrante sostanziale, costituisce un elenco dei principali eventi rischiosi che possono determinare la violazione dei dati e rileva, dalla prospettiva degli interessati, la gravità e la correlata motivazione.
Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679
Fanno parte del sistema di protezione le Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679, le quali vengono allegate al presente documento per formarne parte integrante sostanziale.

SCHEDE DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)
Fanno parte del sistema di protezione le Schede di valutazione di impatto sulla protezione dei dati (DPIA) che esaminano i trattamenti che presentano rischi elevati, le quali vengono allegate al presente documento per formarne parte integrante sostanziale.

SCHEDE DI SINTESI DELLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) PER LA PUBBLICAZIONE
Fanno parte del sistema di protezione le Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente.

MAPPA MISURE DI SICUREZZA LOGISTICHE/FISICHE
Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza logistiche/fisiche.

MAPPA MISURE DI SICUREZZA INFORMATICHE/LOGICHE

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza informatiche/logiche.

MAPPA MISURE DI SICUREZZA ORGANIZZATIVE

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza organizzative

MAPPA MISURE DI SICUREZZA PROCEDURALI

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza procedurali.

ELENCO MISURE DI SICUREZZA

Fa parte integrante e sostanziale del sistema di protezione l'allegato ELENCO misure di sicurezza, correlate alla ricognizione/indice dei trattamenti e suddivise per uffici.

Registro delle attività di trattamento e delle categorie di attività

Fanno parte integrante sostanziale del sistema di protezione:

- il Registro delle attività di trattamento svolte sotto la responsabilità del titolare;
- il Registro del responsabile del trattamento contenente tutte le categorie di attività relative al trattamento svolte per conto del titolare.

ALTRI DOCUMENTI DEL SISTEMA DI PROTEZIONE

Costituiscono parte del sistema di protezione, per formarne parte integrante sostanziale:

- atti di delega al trattamento dei dati;
- atti di nomina degli incaricati.

Costituiscono parte del sistema di protezione, quand'anche non fisicamente allegati al presente documento, i seguenti ulteriori documenti:

- elenco misure minime ITC e relative implementazioni, adottato entro il 31 dicembre 2017;
- GDPR sulla protezione dei dati laddove approvato;
- piano di formazione in materia di diritti e di liberta' delle persone e di protezione dei dati personali per i soggetti autorizzati al trattamento e per incaricati del back up;
- contratti/clausole contrattuali con i responsabili del trattamento;
- pareri del Responsabile protezione dati;
- verbali di vigilanza del responsabile protezione dati;
- circolari;
- informazioni fornite al pubblico e agli interessati;
- altra documentazione utile a comprovare la conformita' dei trattamenti al GDPR e alla normativa interna di adeguamento.

Contesto esterno: trattamenti affidati in outsourcing o effettuati da responsabili esterni

L'Elenco trattamenti affidati in outsourcing o comunque effettuati da responsabili esterni, e allegato al presente documento per formarne parte integrante sostanziale, consente di rilevare il rischio derivante dai trattamenti effettuate, nel contesto esterno alla struttura organizzativa del titolare.

PARTE II

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA VALUTAZIONE

Determinazione di assoggettabilità dei trattamenti a valutazione di impatto – DPIA

In base alla Norma UNI ISO 31.000, la valutazione del rischio richiede l'identificazione, l'analisi e la ponderazione del rischio medesimo.

Ai fini della valutazione del rischio, il GDPR introduce l'obbligo di valutazione d'impatto del trattamento sulla protezione dei dati.

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonchè a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i

requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del GDPR.
Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme ISO (31000 e 27001), dei principi contenuti nel Modello (framework) per la gestione dell'ITC-Information and Communication Technology (modello COBITS) nonchè degli orientamenti contenuti nelle Linee guida e, in particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del GDPR
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1, art. 35 del GDPR;
d) le 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 conformita' al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

RISCHI RESIDUI E CONSULTAZIONE AUTORITÀ DI CONTROLLO
E' nei casi in cui il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati) che questi deve consultare l'autorità di controllo.
Un esempio di un rischio residuo elevato inaccettabile include casi in cui gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poichè non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilita' ben nota).

PARTE III

GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DEL TRATTAMENTO

MISURE DI SICUREZZA DEL TRATTAMENTO
Il GDPR prevede che il titolare del trattamento attui misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1).
L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei 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.
L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

MISURE DI SICUREZZA LOGISTICHE/FISICHE
Sicurezza di aree e locali
L'identificazione delle misure di sicurezza logistiche/fisiche deve tenere conto almeno dei sotto indicati elementi di rischio, indicati a titolo esemplificativo e non esaustivo:

a) Collocazione
- Zona sismica
- Corsi d'acqua nelle vicinanze con rischio esondazione
- Aziende vicine con lavorazioni pericolose
- Installazioni vicine pericolose (aeroporti, depositi carburanti...)
- Area degradata
b) Vicinanza servizi
- Carabinieri o altre forze di polizia e vigilanza
- Ospedali o altri presidi
- Vigili del fuoco
c) Misure presenti anti intrusione
- Antifurto
- Vigilanza
- Videosorveglianza
- Controllo accessi
- Recinzioni
- Cancelli
d) Misure presenti anti incendio
- Estintori
- Idranti
- Rilevatori
d) Misure presenti per la regolarità degli impianti
- Elettrico
- Climatizzazione
- Riscaldamento
e) Misure presenti per la continuità elettrica
- UPS
- Generatori
f) Procedure
- Procedura di gestione degli accessi
- Procedura di gestione dei visitatori/manutentori

L'identificazione delle misure di sicurezza logistiche/fisiche prende in considerazione almeno le principali sotto indicate misure, elencate a titolo esemplificativo e non esaustivo:

a) antifurto
- Sensori
- Allarmi
- Connessione con le forze dell'ordine
- Connessione con servizi di vigilanza
- Videosorveglianza
- Porta normale
- Porta blindata
- Serratura di sicurezza
- Finestre con grate
- Finestre senza grate
b) antincendio
- Sensori
- Allarmi
- Estintori/Impianto antincendio
- Impianti a norma
- Porta taglia fuoco
- Porta antincendio per fuga
- Utilizzo materiale ignifugo
c) Sicurezza ambientale
- Piano di emergenza per la gestione dei rischi individuati
d) Sicurezza accessi

- Controllo
- Registrazione
- Altro

e) Sicurezza CED
- Adeguato posizionamento all'interno dell'edificio
- Adeguate pareti soffitto/pavimento
- Misure anti effrazione
- Controllo accessi
- Impianto di climatizzazione
- Misure antincendio idonee all'uso con le apparecchiature presenti
- Porte antincendio di adeguata dimensione
- Rilevatori di fumo, calore, allagamento

f) continuità operativa
- Gruppo di continuità
- Gruppo elettrogeno
- Coerenza fra i dispositivi di continuita' e le normative VVFF
- Pavimento galleggiante per l'adeguato posizionamento dei cavi
- Corretto ed ordinato posizionamento dei cavi elettrici
- Corretto ed ordinato posizionamento dei cavi di rete
- Posizionamento ordinato delle apparecchiature nei rack
- Spazio intorno ai rack adeguato per la movimentazione e manutenzione delle apparecchiature

g) Sistema di custodia archivi cartacei
- Armadi blindati
- Armadi ignifughi con serratura
- Armadi ignifughi senza serratura
- Altri armadi con serratura
- Altri armadi senza serratura
- Classificatori/cassetti con serratura
- Classificatori/cassetti senza serratura
- Cassaforte
- Scaffalature

La MAPPA delle misure delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

MISURE DI SICUREZZA INFORMATICHE/LOGICHE

Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate per contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in adeguamento della Direttiva 01.08.2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 05.05.2017) della Circolare 18.04.2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 01.08.2015)", le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni.

L'adeguamento dell'Ente alle Misure minime è avvenuto entro il 31.12.2017, come da documentazione in atti che si allega al presente piano per farne parte integrante e sostanziale.

Le Misure, che si articolano sull'adeguamento di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di adeguamento. Il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

Fra le misure minime è previsto anche:
- che le pubbliche amministrazioni accedano sistematicamente a servizi di early warning che consentano loro di rimanere aggiornate sulle nuove vulnerabilità di sicurezza. A tal proposito il CERT-PA fornisce servizi proattivi ed informativi a tutte le amministrazioni accreditate.
Per l'identificazione delle misure minime informatiche/logiche, per la sicurezza ICT ai fini del presente PPD si rinvia alle suddette misure minime per la sicurezza ICT delle pubbliche amministrazioni come attuate e implementate dal titolare.
La MAPPA delle misure delle misure di sicurezza logistiche/fisiche applicate i diversi trattamenti inclusi i criteri e modalità di salvataggio e di ripristino della disponibilità dei dati, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.
Misure di sicurezza organizzative
A titolo esemplificativo e non esaustivo, si elencano:
a) all'individuazione dell'ambito del trattamento consentito ai singoli incaricati
b) alle istruzioni da impartire agli incaricati medesimi
c) al controllo, alla custodia e restituzione della documentazione
d) al controllo degli accessi degli archivi/banche dati";
- esercizio diritti: misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati";
- formazione: formazione di tutti i soggetti che trattano dati personali sotto l'autorità del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli stati membri;
- gestione dati: distruzione documenti non necessari;
- gestione dati: misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonchè necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del garante";
- gestione dati: separazione documenti e dati;
- gestione dati: utilizzazione documenti;
- informazione: informazione continua e aggiornamento costante su procedure operative e istruzioni;
- prescrizioni: nell'attività di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti autorità Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello";
- trattamenti senza l'uso di strumenti elettronici: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
La MAPPA delle misure delle misure di sicurezza organizzative, applicate ai diversi trattamenti allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.
Misure di sicurezza procedurali
Le misure di sicurezza organizzative sono identificate in base ai contenuti e indicazioni del GDPR.
A titolo esemplificativo e non esaustivo, si elencano:
- definizione e attuazione procedura operativa per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilità e la completezza del riscontro fornito agli interessati";
- definizione e attuazione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante";
- definizione e attuazione procedura operativa per il ripristino tempestivo della disponibilita' e l'accesso dei dati personali in caso di incidente fisico o tecnico";
- definizione e attuazione procedura operativa per la pseudonimizzazione e cifratura dei dati personali";

- definizione e attuazione procedura operativa per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati";
- definizione e attuazione procedura operativa per modalità di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 02.07.2015";
- definizione e attuazione procedura operativa per testare, verificare e valutare regolarmente l'efficacia:
a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
b) le misure di ripristino in caso di "data breach";
- definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.L.vo 196/2003 per i trattamenti con strumenti diversi da quelli elettronici:
a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi;
c) le modalita' del controllo, custodia e restituzione della documentazione;
d) le modalita' del controllo degli accessi agli archivi/banche dati";
- definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonché per documentare i provvedimenti adottati per porvi rimedio nonchè per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi";
- definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto:
a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali;
b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del GDPR".
La MAPPA delle misure di sicurezza procedurali, applicate ai diversi trattamenti è allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

PIANO FORMATIVO

Il piano formativo deve essere impostato sulla Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le libertà delle persone fisiche e sulla protezione di tali diritti e libertà, con particolare riferimento al diritto alla protezione dei dati personali;

Codici di condotta

Per i codici di condotta si rinvia ai codici approvati dal Garante.

Certificazione

Si rinvia alla certificazione eventualmente acquisita per formare parte integrante e sostanziale del presente PPD.

Notifica di una violazione dei dati personali all'Autorità di controllo

Per le notifiche all'Autorità di controllo, il presente PPD rinvia alla definizione e attuazione di adeguate misure organizzative e procedurali, ferma restando la disciplina del GDPR.

Comunicazione di una violazione dei dati personali all'interessato

Per la comunicazione di una violazione dei dati personali all'interessato, il presente PPD rinvia alla definizione e attuazione di adeguate misure organizzative e procedurali, ferma restando la disciplina del GDPR.

ALLEGATI

01 - MAPPA STRUTTURA ORGANIZZATIVA ED ELENCO SOGGETTI INTERNI ED ESTERNI
02 - SCHEDE DI RICOGNIZIONE TRATTAMENTI ED ELENCO TRATTAMENTI E SCHEDE DPIA
03 - MAPPA DEI LUOGHI
04 - MAPPA HARDWARE, SOFTWARE CON INDICAZIONE DEGLI ARCHIVI E BANCHE DATI ELETTRONICHE
05 - MAPPA RISCHI E MOTIVAZIONI DI STIMA
06 - MAPPA MISURE DI SICUREZZA
07 - PROGRAMMAZIONE CORSI DI FORMAZIONE