COMUNE DI MANTOVA

PIANO DI PROTEZIONE DEI DATI PERSONALI
E GESTIONE DEL RISCHIO DI VIOLAZIONE[1]
per una gestione del rischio robusta

approvato 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 personali e gestione del rischio di violazione**

Numero di versione: **3**

Data ultimo aggiornamento: **11/09/2026**

Stato del documento: **Approvato dal Titolare con proprio provvedimento**

Estensori del documento: **Titolare del trattamento con il supporto del RPD**

Riferimento per comunicazioni in merito al documento: **comune.mantova.aoo@legalmail.it**

Modalita' di distribuzione del presente documento e delle eventuali nuove versioni: **Pubblicazione, anche per estratto, sul sito web istituzionale nella sezione Amministrazione Trasparente**

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e'' 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 autorita' pubbliche. Senonche', la rapidita' 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 aprile 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 virtu' 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 Protezione 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 attivita' 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.
In tale quadro, il documento disciplina, secondo i principi della NORMA UNI ISO 31000, il processo di gestione del trattamento dei dati personali e il rischio di violazione dei dati personali medesimi.

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 affinche' 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.Lgs. n.196/2003);

- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 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;

- D.Lgs. 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 (Giunta Comunale) dell'intestato titolare ha approvato il PPD con provvedimento nr. …. del ……..

PERIODO DI RIFERIMENTO E MODALITA' DI AGGIORNAMENTO

Il PPD copre il periodo del triennio 2026-2028, e la funzione principale dello stesso e' 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 piu' incisivi.

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:

- dirigenti/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 e all'OIV.

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 rapidita' dell'evoluzione tecnologica nonche' la globalizzazione comportano nuove sfide per la protezione dei dati personali. Sempre piu' 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 e' aumentata in modo significativo. Tale evoluzione richiede un quadro piu' solido e coerente in materia di protezione dei dati, tenuto conto dell'aumento del rischio di violazione dei dati medesimi e della necessita' che le persone fisiche abbiano il controllo dei dati personali che li riguardano in un quadro di certezza giuridica e operativa rafforzata cosi' come delineata del GDPR.
Il rischio inerente al trattamento e' 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'autorita' di controllo competente per ottenere indicazioni su come gestire il rischio residuale, fermo restando che l'autorita' 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 documentate almeno da:

- Piano protezione dati -PPD;

- Registri delle attivita' e delle categorie dei trattamenti (prot. 68398/2026);

- Mappa struttura organizzativa (Allegato 1);

- Mappa dei soggetti (Allegato 1);

- Mappa dei luoghi (Allegato 3);

- Schede di ricognizione dei trattamenti (in atti) - Mappa dei trattamenti (Allegato 2);

- Mappa hardware (Allegato 4);

- Mappa software (Allegato 4);

- Mappa rischi e motivazioni stima (Allegato 5);

- Schede di determinazione preliminare della possibilita' 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 (in atti prot. 106130/2026) e a rischio non elevato (in atti prot. 106134/2026);

- Mappa delle misure di sicurezza logistiche/fisiche (Allegato 6);

- Mappa delle misure di sicurezza informatiche/logiche (Allegato 6);

- Mappa delle misure di sicurezza organizzative (Allegato 6);

- Mappa delle misure di sicurezza e procedurali (Allegato 6);

- 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 gravita' e probabilita'.

- la nozione di "gestione dei rischi" come l'insieme delle attivita' 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 liberta' 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 liberta'" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la liberta' di parola, la liberta' di pensiero, la liberta' di circolazione, il divieto di discriminazione, il diritto alla liberta' di coscienza e di religione.

I documenti allegati e, in particolare, la ricognizione dei trattamenti in rapporto a tutta l'attivita' dell'ente, le schede di DPIA e l'elenco dei rischi, della gravita' 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: **Comune di Mantova**

Sede: **Via Roma 39, 46100 Mantova**

Punti di contatto: Tel. **0376.3381** PEC: **comune.mantova.aoo@legalmail.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 piu' altri titolari del trattamento determinano congiuntamente le finalita' e i mezzi del trattamento.

I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilita' 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'opportunita' 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 il responsabile del trattamento, o chiunque agisca sotto la sua autorita' o sotto quella del titolare del trattamento, che abbia accesso a dati personali puo' 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.Lgs. 30 giugno 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'attivita' 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, altresi', 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 gravita' e la correlata motivazione.

Schede di determinazione preliminare della possibilita' 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 possibilita' 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.

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 attivita'

Fanno parte integrante sostanziale del sistema di protezione:

- il Registro delle attivita' di trattamento svolte sotto la responsabilità del titolare;

- il Registro del responsabile del trattamento contenente tutte le categorie di attivita' 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 III
GESTIONE DEL RISCHIO SECONDO LA NORMA UNI ISO 31.000: FASE DELLA VALUTAZIONE

Determinazione di assoggettabilita' 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 e' un processo inteso a descrivere il trattamento, valutarne la necessita' e la proporzionalita', nonche' 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) nonche' 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 finalita' del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessita' e proporzionalita' dei trattamenti in relazione alle finalita';

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 Autorita' 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'autorita' 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 verifichera' (ad esempio: poiche' non si e' in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalita' di condivisione, utilizzo o distribuzione o quando non si puo' porre rimedio a una vulnerabilità ben nota).

PARTE IV
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 probabilita' e gravita' diverse per i diritti e le liberta' 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 puo' essere utilizzata come elemento per dimostrare la conformita' ai requisiti di cui al paragrafo 1 del presente articolo.

Il titolare del trattamento e il responsabile del trattamento fanno si' che chiunque agisca sotto la loro autorita' e abbia accesso a dati personali non tratti tali dati se non e' 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 sottoindicati elementi di rischio, indicati a titolo esemplificativo e non esaustivo:

a) <u>Collocazione</u>

- Zona sismica
- Corsi d'acqua nelle vicinanze con rischio esondazione
- Aziende vicine con lavorazioni pericolose
- Installazioni vicine pericolose (aeroporti, depositi carburanti...)
- Area degradata

b) <u>Vicinanza servizi</u>

- Carabinieri o altre forze di polizia e vigilanza
- Ospedali o altri presidi
- Vigili del fuoco

c) <u>Misure presenti antintrusione</u>

- Antifurto

- Vigilanza
- Videosorveglianza
- Controllo accessi
- Recinzioni
- Cancelli

d) Misure presenti antincendio

- Estintori
- Idranti
- Rilevatori

d) Misure presenti per la regolarita' degli impianti

- Elettrico
- Climatizzazione
- Riscaldamento

e) Misure presenti per la continuita' 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 sottoindicate 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 antieffrazione
- 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 continuita'

- 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 piu' comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in adeguamento della Direttiva 1 agosto 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 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del

Presidente del Consiglio dei ministri 1° agosto 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 dicembre 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 piu' completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticita' 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 vulnerabilita' 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 modalita' di salvataggio e di ripristino della disponibilita' 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'intelligibilita' e la completezza del riscontro fornito agli interessati";

- formazione: formazione di tutti i soggetti che trattano dati personali sotto l'autorita' 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 nonche' 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'attivita' di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti autorita' 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 i 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'intelligibilita' 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 modalita' di accesso finalizzata all'identificazione degli incaricati";

- definizione e attuazione procedura operativa per modalita' di scambio dei dati personali tra amministrazioni pubbliche definitivamente nel provvedimento del Garante n. 393 del 2 luglio 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.Lgs. 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, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' 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 e' 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 di 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 liberta', 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'Autorita' di controllo
Per le notifiche all'Autorita' 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 DEI TRATTAMENTI / MAPPA DEI TRATTAMENTI

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