**PIANO DI PROTEZIONE DEI DATI PERSONALI**

**E GESTIONE DEL RISCHIO DI VIOLAZIONE**

**DPIA- FASE 2**

**VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI - DPIA[[1]](#footnote-1)**

Documento per provare ed essere in grado di dimostrare che

il trattamento e' effettuato conformemente al RGPD

|  |  |
| --- | --- |
| **SETTORE** | FINANZIARIO |
| **SERVIZIO** | RAGIONERIA |
| **UFFICIO** | Ragioneria |

|  |  |
| --- | --- |
| **TRATTAMENTO** | Nessun trattamento - Assenza dati personali da trattare |

|  |  |
| --- | --- |
| **Abbinamento del trattamento ad un insieme di trattamenti simili** | La Scheda in esame **raggruppa** una pluralita' di procedimenti/processi di competenza dell'Ufficio. Per alcuni di tali procedimenti/processi, la Scheda di trattamento si adatta in tutte le sue parti. Per altri procedimenti/processi, per contro, la Scheda di trattamento in esame si adatta solo in parte, per quanto concerne la *Fonte normativa, le Rilevanti finalita' di interesse pubblico perseguite dal trattamento, il Trattamento "ordinario" dei dati e la Sintetica descrizione del trattamento e del flusso informativo*.  Ai soli fini della valutazione di impatto, la Scheda di trattamento in esame viene comunque **abbinata e utilizzata** per tutti i procedimenti/processi che presentano **trattamenti simili** con rischi analoghi, in attuazione di quanto indicato dalle *Linee guida sulla valutazione di impatto* secondo cui la valutazione può essere effettuata per un **insieme di trattamenti simili** ovvero per un **insieme di trattamenti multipli simili**.  L'elenco dei procedimenti/processi che presentano trattamenti simili, con rischi analoghi, e' contenuto in calce al presente documento. |

|  |  |
| --- | --- |
| **Titolo del Documento** |  |
| **Numero di versione** | 001 |
| **Data ultimo aggiornamento** | 30/04/2020 |
| **Stato del documento** | Approvato dal titolare con proprio provvedimento |
| **Estensori del documento** | - Titolare del trattamento |
| **Riferimento per comunicazioni in merito al documento** | - Punti di contatto del titolare del trattamento - TTD |
| **Modalita' di distribuzione del presente documento e delle eventuali nuove versioni** | - Trasmissione tramite la rete intranet  - Conservazione con supporto informatico |

**RISCHIO ELEVATO E OBBLIGO DI DPIA**

In base alla determinazione di assoggettabilita' a valutazione di impattato (DPIA), il trattamento in epigrafe indicato, sulla base dei CRITERI in relazione alle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto ai sensi dell'Allegato 1 al provvedimento n. 467/2018 del Garante, presenta un **elevato rischio** per i diritti e le liberta' delle persone fisiche, e non rientra tra le eccezioni per le quali non e' obbligatorio svolgere la valutazione di impatto sulla protezione dei dati (di seguito solo "DPIA") ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (di seguito solo "RGPD").

La determinazione sulla possibilita' di un rischio elevato risulta documentata in atti (Fase 1 DPIA) dalla **RELAZIONE/REPORT** sulla possibilita' che il trattamento possa presentate un tale rischio, elaborata conformemente alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilita' che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 ( di seguito solo "Linee guida") e in relazione al provvedimento n. 467/2018 del Garante.

La DPIA viene condotta secondo lo schema sotto riportato, e desunto dalle Linee guida in precedenza citate.



Il presente documento ha la funzione di garantire la **tracciabilita' documentale** della DPIA relativamente al trattamento in epigrafe indicato, al fine di consentire al titolare di provare la conformita' al RGPD in caso di richiesta dell'Autorita' di controllo.

**OBIETTIVI DA RAGGIUNGERE**

La DPIA e' funzionale alla gestione del rischio[[2]](#footnote-2), per tale intendendosi il complesso delle attivita' coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.

L'art. 35 RGPD fa riferimento al possibile rischio elevato "*per i diritti e le liberta' delle persone fisiche*". 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.

In questo quadro, la DPIA intende fungere da strumento:

* che consente di ridurre il rischio del trattamento in esame ad un livello accettabile, configurandosi come un processo continuo e dinamico;
* che consente di comprovare la conformita' del sistema al RGPD.

**DEFINIZIONE E DOCUMENTAZIONE DEI RUOLI**

I ruoli, nello svolgimento della DPIA relativa al trattamento in epigrafe indicato, tengono conto di quanto stabilito nelle Linee guida. In particolare:

a) **il titolare del trattamento**:

* assicura che la DPIA sia eseguita, e che venga effettuata la consultazione con il responsabile della protezione dei dati (RPD) e che il parere ricevuto, cosi' come le decisioni prese dal titolare medesimo, risultano documentate all'interno della DPIA
* raccoglie le opinioni degli interessati o dei loro rappresentanti e, qualora la decisione finale si discosti dalle opinioni degli interessati, assicura che le motivazioni a sostegno della decisione risultino documentate
* documenta, altresi', la giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che cio' non sia appropriato
* se del caso, consulta esperti indipendenti che esercitano professioni diverse (avvocati, sociologi, esperti di etica, esperti informatici, esperti di sistemi di sicurezza, etc.)
* sorveglia lo svolgimento della valutazione d'impatto sulla protezione dei dati e ne assicura la tracciabilita' documentale

b) **il responsabile del trattamento dei dati**, qualora il trattamento venga eseguito in toto o in parte da quest'ultimo:

* assiste il titolare del trattamento nell'esecuzione della DPIA e fornisce tutte le informazioni necessarie

c) **il responsabile della protezione dei dati** e **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato,** suggeriscono al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento, assistono le parti interessate in relazione alla metodologia, contribuiscono alla valutazione della qualita' della valutazione dei rischi e del grado di accettabilita' del rischio residuo, nonche' allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;

d) **il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione**, dovrebbero fornire assistenza al titolare del trattamento, nonche' potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza

**CONTENUTI MINIMI E METODOLOGIA PER LO SVOLGIMENTO DELLA DPIA**

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 RGPD :

|  |  |
| --- | --- |
| 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 liberta' degli interessati di cui al paragrafo 1; e |

|  |  |
| --- | --- |
| 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. |

Lo schema che segue, desunto dalle Linee guida, indica il processo iterativo per lo svolgimento della DPIA.



In attuazione della descritta metodologia e workflow, la **RELAZIONE/REPORT** sullo svolgimento della DPIA relativa al trattamento in epigrafe indicato, e da utilizzare per provare la conformita' al RGPD, e' la seguente.

**SEZIONE I**

**DESCRIZIONE SISTEMATICA**

**DEL TRATTAMENTO PREVISTO E DELLE FINALITA'**

**compreso, ove applicabile, l'interesse legittimo perseguito dal titolare**

**(art. 35, paragrafo 7, lettera a)**

|  |  |
| --- | --- |
| **SETTORE** | FINANZIARIO |
| **SERVIZIO** | RAGIONERIA |
| **UFFICIO:** denominazione e punti di contatto | Ragioneria |
| **Titolare trattamento:** denominazione e punti di contatto | Comune di VETTO  Sindaco Ruffini Fabio Tel. 0522 815221  Email: sindaco@comune.vetto.re.it |
| **Contitolare/i trattamento:** denominazione e punti di contatto |  |
| **Responsabile trattamento:** denominazione e punti di contatto |  |
| **Sub-Responsabile:** denominazione e punti di contatto |  |
| **Delegato trattamento:** denominazione e punti di contatto | Dott. Favali Federico |
| **Incaricati trattamento:** denominazione e punti di contatto | Ruffini Barbara  Zampineti Monica |

|  |
| --- |
| **Sintetica descrizione del trattamento e del flusso informativo** |

|  |  |  |
| --- | --- | --- |
| **RGPD** | | **FRAMEWORKS FUNZIONE** |
| art.35 lett.a) | | Descrivere |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** | |
| **Fonte normativa** |  | |
| **Natura del trattamento** |  | |
| **Ambito di applicazione del trattamento** |  | |
| **Nome archivio/Banca dati** |  | |
| **Tipo di archivio/Banca dati** |  | |
| **Categorie-tipi di dati** |  | |
| **Luoghi di custodia dei dati** |  | |
| **Finalita' del trattamento** |  | |
| **Rilevanti finalita' di interesse pubblico** |  | |
| **Interesse legittimo perseguito** |  | |
| **Categorie di trattamenti- forme ordinarie di elaborazione** |  | |
| **Categorie di trattamenti - particolari forme di elaborazione: *comunicazione*** |  | |
| **Categorie di trattamenti - particolari forme di elaborazione: *diffusione*** |  | |
| **Categorie di trattamenti - particolari forme di elaborazione: *trasferimento all'estero*** |  | |
| **Categorie di trattamenti - particolari forme di elaborazione:** ***trattamento effettuato tramite un sito web-nome del dominio del sito web*** |  | |
| **Categorie di trattamenti - particolari forme di elaborazione:** ***trattamento effettuato tramite un sito web-Paese/i di ubicazione del/i server*** |  | |
| **Categorie di interessati** |  | |
| **Categorie di destinatari** |  | |
| **Strumenti e risorse coinvolti nel trattamento dei dati personali: *hardware, software, reti, persone, supporti cartacei o canali di trasmissione*** | Gli strumenti e le risorse coinvolti nel trattamento dei dati personali e, in particolare, gli hardware, i software, le reti, le persone, i supporti cartacei o canali di trasmissione sono analiticamente elencati nella MAPPA DEI SINGOLI UFFICI che effettuano il trattamento allegata, e a cui si rinvia | |
| **Strumenti e risorse coinvolti nel trattamento dei dati personali: *uso nuove tecnologie*** |  | |
| **Cessazione trattamento: *Periodo di conservazione dei dati*** |  | |
| **Cessazione trattamento: *termine ultimo per la cancellazione delle diverse categorie di dati*** |  | |
| **Cessazione trattamento: *modalita' di cessazione dei dati*** |  | |
| **Parere RPO/RTD** |  | |
| **Opinioni interessati o loro rappresentanti** |  | |
| **Rispetto codici di condotta approvati** |  | |
| **Adesione ad un meccanismo di certificazione** |  | |
| **Registrazione dei dati personali, dei destinatari e del periodo di conservazione dei dati personali** |  | |

**SEZIONE II**

**VALUTAZIONE DELLA NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO**

**E MISURE PREVISTE PER DIMOSTRARE LA CONFORMITA' AL RGPD**

**(art. 35, paragrafo 7, lettera b)**

1. **NECESSITA' E PROPORZIONALITA' DEL TRATTAMENTO**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| **art**.35 lett.b) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Misure che contribuiscono alla proporzionalita' e necessita' del trattamento in relazione alle finalita'** |  |
| **Misure che contribuiscono ai diritti degli interessati in relazione alle finalita'** |  |

**A) CONFORMITA' RGPD**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.35 lett.d) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Misure previste per dimostrare la conformita' al RGPD** |  |

**SEZIONE III**

**VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI E MISURE DI SICUREZZA PREVISTE PER AFFRONTARE I RISCHI**

**(art. 35, paragrafo 7, lettera c)**

**A) RISCHI**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.35 lett.c) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **RISCHI**  **Origine/fonte dei rischi: *accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati***  (rilevati dalla prospettiva degli interessati) |  |
| **RISCHI**  **Impatti potenziali in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilita' dei dati**  (rilevati dalla prospettiva degli interessati) |  |
| **Minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilita' dei dati**  (rilevati dalla prospettiva degli interessati) |  |
| **PROBABILITA' = X**  (rilevata dalla prospettiva degli interessati) |  |
| **GRAVITA' = Y**  (rilevata dalla prospettiva degli interessati) |  |
| **STIMA (XxY)**  **DELLA PROBABILITA' E GRAVITA'**  (rilevata dalla prospettiva degli interessati) |  |

**MATRICE UTILIZZATA PER IL CALCOLO DELLA STIMA**

* Per ogni trattamento sono state definite ed identificate le diverse componenti dei rischi, e precisamente:
* - **MINACCE**, quali **eventi** che possono provocare un danno ai dati, nel caso si verifichino;

- **livello delle minacce**, quale **probabilita'** (riportata in valori da 1 a 4) che si verifichi la minaccia, prima della adozione delle contromisure;

* + - *1 = basso-trascurabile* = e' **molto improbabile** che la minaccia si possa verificare
    - *2 = medio =* e' **improbabile** che la minaccia si possa verificare
    - *3 = alto* = *=* e' **probabile** che la minaccia si possa verificare
    - *4 = molto alto =* e' **altamente probabile** che la minaccia si possa verificare
  + **- IMPATTO,** quale conseguenza del verificarsi di una minaccia e, quindi del verificarsi dell'evento dannoso sui dati
  + - **livello dell'impatto**, quale quantificazione, in termini di **gravita'**, del danno (in **una scala da 1 a 4**) valutato sia da un punto di vista quantitativo (costi di ripristino, giornate di lavoro ...) che da un punto di vista qualitativo (perdita di immagine, violazioni, perdita di operativita' ...).
    - *1 = basso-trascurabile*
    - *2 = medio*
    - *3 = alto*
    - *4 = molto alto*
    - La funzione di rischio adottata si basa su una matrice di valutazione del rischio che fornisce un **valore nel range 1:16** in funzione delle minacce e dell'impatto con i seguenti risultati:

**Valore del rischio da 1 a 2 = RISCHIO BASSO** (verde)

**Valore del rischio da 3 a 4 = RISCHIO MEDIO** (giallo)

**Valore del rischio da 6 a 9 = RISCHIO ALTO** (arancione)

**Valore del rischio da 12 a 16 = RISCHIO ALTISSIMO** (rosso)

* + 

La stima del rischio costituisce l'input per definire e selezionare:

* le politiche di sicurezza
* le misure per ridurre il rischio ad un livello considerato accettabile

In funzione della stima del rischio**,** il titolare adotta **misure di sicurezza adeguate** per salvaguardare il diritto di protezione dei dati pianificando, anche ai fini del monitoraggio, le **priorita' e attuazione delle stesse**.

**B) MISURE DI SICUREZZA PREVISTE PER GESTIRE I RISCHI**

|  |  |  |
| --- | --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** | **RISCHI CONTRASTATI** |
| art.35 lett.c) | **Proteggere** | Come da MAPPA dei rischi contrastati |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** | |
| **Misure di sicurezza:**  **tecniche logistiche** |  | |
| **Misure di sicurezza:**  **tecniche informatiche, comprese le misure di ripristino in caso di data breach** |  | |
| **Misure di sicurezza:**  **Organizzative** |  | |
| **Misure di sicurezza:**  **procedurali** |  | |

**C) RISCHIO RESIDUO**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.36 lett.c) | **Valutare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Livello rischio dopo l'applicazione delle misure** |  |

**D) CONSULTAZIONE PREVENTIVA PER RISCHIO RESIDUO ELEVATO O NEI CASI IMPOSTI DALLA LEGGE**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS FUNZIONE** |
| art.36 | **Consultare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
|  |  |

**SEZIONE IV**

**DOCUMENTAZIONE**

**(art. 24, paragrafo 1)**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS**  **FUNZIONE** |
| art.24 | **Documentare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Documentare la conformita' al RGPD** |  |

**SEZIONE IV**

**MONITORAGGIO E RIESAME DPIA**

**( art. 35, paragrafo 11)**

|  |  |
| --- | --- |
| **RGPD** | **FRAMEWORKS**  **FUNZIONE** |
| art. 35 | **Monitorare** |
| **CRITERI**  **LINEE GUIDA** | **DPIA**  **TRATTAMENTO** |
| **Stato attuazione misure** | - Parzialmente attuate |
| **Fasi attuazione misure** | - Comunicazione e trasmissione misure ai soggetti tenuti all'attuazione: FASE 1  - Informazione e formazione dei soggetti tenuti all'attuazione: FASE 3  - Realizzazione azioni ricomprese nelle misure da parte dei soggetti tenuti all'attuazione: FASE 2  - Reportistica e monitoraggio attuazione misure e eventuali azioni correttive: FASE 4 |
| **Indicatori attuazione misure** | - Percentuale significativa di azioni attuate sul numero programmato  - Percentuale significativa di interventi di comunicazione e trasmissione ai soggetti tenuti all'attuazione sul numero programmato  - Percentuale significativa di interventi di informazione e formazione dei soggetti tenuti all'attuazione sul numero programmato  - Percentuale significativa di report e monitoraggi eseguiti sul numero programmato |
| **Responsabile attuazione misure** | Delegato interno |

|  |  |  |
| --- | --- | --- |
| **RIESAME DPIA** | | |
| **Motivazione riesame** | - La determinazione di assoggettabilita' a DPIA e il presente documento sono costantemente sottoposti a riesame, documentati dal numero della versione e dalla relativa data, in relazione ai mutamenti di contesto |

|  |
| --- |
| **ELENCO DEI TRATTAMENTI**  **INSERITI NELL'INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ANALOGHI/ INSIEME DI TRATTAMENTI MULTIPLI SIMILI** |

1. Conforme alle Linee guida del Garante, Allegato 2 "Criteri per una valutazione d'impatto sulla protezione dei dati accettabile" [↑](#footnote-ref-1)
2. Al fine di poter gestire i rischi per i diritti e le liberta' delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. Il titolare del trattamento non puo' per contro sottrarsi alla responsabilita' coprendo i rischi stipulando polizze assicurative. [↑](#footnote-ref-2)