Identificativo: D04_SCO.1_FASE1(ALL3) Rev. 1.0

Data: 23/03/2021

PROCEDURA RISTRETTA PER L'AFFIDAMENTO DEI SERVIZI DI CLOUD COMPUTING, DI SICUREZZA, DI REALIZZAZIONE DI PORTALI E SERVIZI ON-LINE E DI COOPERAZIONE APPLICATIVA PER LE PUBBLICHE AMMINISTRAZIONI (ID SIGEF 1403)

LOTTO 2

CIG 8025774638

Regione Calabria

Modello Report DPIA

Allegato 3 del deliverable D04_SCO.1_FASE1 "Metodologia della valutazione d'impatto per la protezione dei dati personali (DPIA)"

Raggruppamento Temporaneo di Imprese

composto da:

Leonardo Divisione Cyber Security SpA

IBM SpA

Sistemi Informativi SpA

Fastweb SpA

SOMMARIO

1 INTRODUZIONE

Il presente documento presenta il report da predisporre per sintetizzare tutte le risultanze della Valutazione d'impatto delle attività di trattamento (DPIA). Tale report, oltre che a illustrare i risultati ottenuti e dimostrare la corretta esecuzione formale della DPIA e la sua aderenza ai requisiti richiesti dal GDPR, rappresenta anche un efficace strumento per il Delegato del Titolare del trattamento, per tenere sotto controllo i rischi degli interessati e dimostrare (Accountability) di aver agito in modo appropriato per gestirli.

La DPIA è infatti un'attività utile per acquisire piena consapevolezza dei rischi e per selezionare e giustificare le misure tecniche e organizzative necessarie da adottare.

Nel report finale verranno riportati quindi gli elementi fondamentali del trattamento oggetto di DPIA, il risultato della valutazione di impatto che emerge dall'esecuzione dell'analisi del rischio e le decisioni assunte in merito all'esecuzione/non esecuzione del medesimo trattamento. Tutti i risultati ottenuti nell'ambito della DPIA dovranno essere documentati, ponendo particolare cura:

1. nella descrizione sistematica del trattamento;
2. nella valutazione e dimostrazione della necessità e proporzionalità del trattamento;
3. nella valutazione e nelle modalità di gestione dei rischi degli interessati;
4. nell'acquisizione del parere del Responsabile della protezione dei dati (RPD) e, ove opportuno, delle opinioni raccolte a seguito dell'eventuale consultazione pubblica di soggetti esterni.

La relazione finale della DPIA dovrà essere validata dal Team DPIA e sottoscritta dal Delegato del Titolare del trattamento.

2 GLOSSARIO

DEFINIZIONE/ACRONIMO	DESCRIZIONE
Accountability	È richiesto al Titolare di dimostrare, documentalmente, la conformità al GDPR.
Categorie particolari di dati personali	L'Origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Clausole contrattuali standard	Clausole contrattuali che consentono di trasferire dati personali verso Paesi terzi.
Dati personali relativi a condanne penali e reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Decisioni di adeguatezza	Decisioni della Commissione europea che stabilisce, sulla base di un procedimento che prevede, fra l'altro, il parere favorevole del Gruppo ex Articolo 29 della Direttiva 95/46/CE, che il livello di protezione offerto in un determinato Paese Terzo è adeguato e che pertanto è possibile trasferirvi dati personali.
Diffusione	La divulgazione di dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).
DPIA (o PIA)	Data Protection Impact Assessment (o Privacy Impact Assessment): è la valutazione d'impatto sulla protezione dei dati da eseguire in funzione. Tale processo è volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Lo stesso può riguardare una singola operazione di trattamento dei dati, ma potrebbe riferirsi anche a trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.
Interessato	La persona fisica cui si riferiscono i dati personali.

DEFINIZIONE/ACRONIMO	DESCRIZIONE
Liceità del trattamento	Il Trattamento di dati personali può essere considerato lecito se ricorre almeno una delle seguenti condizioni; a) L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità b) Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso c) Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento f) Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
Misure di sicurezza	Insieme degli accorgimenti tecnici, organizzativi o fisici, dei dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, delle misure che permettano alle sole persone autorizzate di avere accesso ai dati; ulteriori accorgimenti atti ad evitare che siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti , ecc.
Norme vincolanti d'impresa	Politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune". Norme vincolanti d'impresa per i titolari del trattamento: BCR-C Norme vincolanti d'impresa per il Responsabile del trattamento: BCR-P
Privacy by design	Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

DEFINIZIONE/ACRONIMO	DESCRIZIONE
Privacy Shield	L'accordo Privacy Shield ("Scudo privacy") fra USA e UE ha introdotto una serie di vincoli ed obblighi stringenti applicabili ai soggetti giuridici statunitensi che trattano dati trasferiti dai Paesi UE. il Garante Privacy italiano, con Provvedimento di autorizzazione del 27 ottobre 2016, ha autorizzato il trasferimento di dati personali dal territorio italiano verso le organizzazioni presenti negli Stati Uniti che figurano nell'elenco degli aderenti al "Privacy Shield".
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Pseudonimizzazione	Trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Titolare del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

3 MODELLO PER LA DOCUMENTAZIONE DELLA VALUTAZIONE DI IMPATTO (DPIA)

NOTA: TUTTE LE PARTI IN CARATTERE ITALICO DI COLORE ROSSO (COMPRESA LA PRESENTE NOTA) RAPPRESENTANO SOLO SUGGERIMENTI DI COMPILAZIONE CHE DOVRANNO ESSERE ELIMINATI NELLA VERSIONE FINALE DEL DOCUMENTO

Nome del Delegato del Titolare per il trattamento

adsdas

Nome del Responsabile della protezione dei dati personali

Componenti del Team[1] DPIA

Denominazione del trattamento

Data ultimo aggiornamento

Frequenza di aggiornamento prevista

3.1 Contesto

3.1.1 Panoramica del trattamento

Descrizione del trattamento

Quale è il trattamento in considerazione? Fornire una breve descrizione del trattamento in esame, la sua natura, le finalità, il contesto, le relative problematiche. Quali sono le responsabilità connesse al trattamento? Identificare gli eventuali Contitolari e collaboratori di riferimento per il trattamento

Descrizione del trattamento	

[1] Oltre al Delegato del Titolare e al RPD.

Finalità	
Descrizione del contesto ed eventuali problematiche	
Contitolare/i	
Funzionario/i di riferimento competente/i del trattamento oggetto di DPIA	

Standard di settore applicabili al trattamento

Ci sono standard applicabili al trattamento? Elencare le regole o gli standard di riferimento applicabili al trattamento, sia utili sia obbligatori, in particolare i codici di condotta approvati (vedi Art. 40 del RGPD e le certificazioni inerenti la protezione dei dati (vedi art. 42 RGPD), le regole deontologiche e le prescrizioni del Garante per la protezione dei dati personali o da altri soggetti competenti ai sensi del d.lgs. 196/2003 (art. 2-quater, art. 2-quinquiesdecies, art. 2-septies, art. 2-octies

Standard applicabili al trattamento	Osservazioni/considerazioni

3.1.2 Dati, processi e risorse di supporto

Questa sezione permette di definire e descrivere nei dettagli il trattamento in esame. Definire e descrivere l'ambito in dettaglio:

- *i dati personali in questione, i loro destinatari e i periodi di conservazione*
- *descrizione dei processi e delle risorse dedicate alla gestione dei dati personali per l'intero ciclo di vita dei dati stessi (dalla raccolta alla cancellazione)*

Descrizione dei dati

Quali sono i dati trattati?

Dati trattati	Destinatari	Periodo di conservazione

Descrizione delle fasi/operazioni di trattamento e delle risorse di supporto

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)? E' raccomandato allegare un diagramma di flusso. Quali sono le risorse di supporto ai dati? Descrivere le risorse su cui si basano i trattamenti dei dati personali. Esse possono comprendere hardware, software, reti, persone, supporti cartacei o documentazione

Fase del trattamento	Descrizione dettagliata delle operazioni svolte in ciascuna fase	Risorse di supporto ai dati

3.2 Principi fondamentali

3.2.1 Proporzionalità e necessità del trattamento

Proporzionalità e necessità

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti

Finalità

Gli scopi del trattamento sono specifici, espliciti, legittimi? Descrizione degli scopi relativi al trattamento dei dati e dimostrazione che questi siano espliciti e legittimi (Art. 5.1 (b) del GDPR)

Finalità	Legittimità

Basi giuridiche

Quali sono le basi giuridiche che rendono legittimo il trattamento? Descrizione delle basi giuridiche di legittimità del trattamento (Art. 6 del GDPR), anche in considerazione dei valori presenti nella tabella e conformità alle prescrizioni che impongono il divieto di trattamento

Base legale	Verificare quale è la fattispecie applicabile	Specificare i riferimenti e motivare

Principio di minimizzazione dei dati

I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? Descrivere e dimostrare di aver dato applicazione al principio; dimostrare che i dati raccolti, suddivisi per categorie, sono adeguati, rilevanti e pertinenti in relazione alla finalità per cui sono stati trattati (Art. 5 (c) del RDGP)

Dettagli inerenti ai dati trattati	Categorie di dati	Dimostrazione della necessità e della rilevanza del dato	Misure di minimizzazione

Principio di qualità dei dati

I dati sono esatti e aggiornati? Descrivere e dimostrare di aver dato applicazione al principio, indicando le misure adottate per cancellare o rettificare tempestivamente i dati personali inesatti rispetto alle finalità per le quali sono trattati (esattezza), in conformità con l'art. 5.1 d) del GDPR

Principio di limitazione della conservazione

Qual è il periodo di conservazione dei dati? Descrivere e dimostrare di aver dato applicazione al principio: dimostrare che il periodo di conservazione è limitato/idoneo ai fini per cui è stato effettuato il trattamento (Art. 5 (e) del RGPD). Deve essere definito un periodo di conservazione per ciascun tipo di dato motivandolo in rapporto alle esigenze del trattamento e/o all'esistenza di vincoli di legge. Occorre distinguere tra dati correnti e dati archiviati, il cui accesso sarà limitato ai soli soggetti interessati. È necessario implementare un meccanismo di soppressione per archiviare i dati correnti o eliminare i dati archiviati al termine del loro periodo di conservazione. Inoltre è necessario eliminare le tracce funzionali e i log tecnici che non possono essere conservati a tempo indeterminato

Tipologia di dato	Periodo di conservazione	Giustificazione del periodo di conservazione	Modalità di cancellazione alla fine del periodo di conservazione
Dati correnti			
Dati archiviati			
Tracce funzionali			
Log tecnici di sistema e altri log tecnologici			

3.2.2 Misure a tutela dei diritti degli interessati

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti

Informazioni agli interessati

Come si vuole informare del trattamento gli interessati? Descrivere quali informazioni s'intende dare e con quali mezzi, previa verifica, della correttezza e la trasparenza dell'informativa relativa al trattamento dei dati personali (Art. 12, 13 e 14 del GDPR) e salva la presenza di esenzioni specifiche riferite al trattamento

Consenso dell'interessato

Ove applicabile: come si ottiene il consenso degli interessati? Descrivere il processo per l'ottenimento del consenso degli interessati: Identificare o determinare come si progetta l'acquisizione del consenso per il trattamento dei dati da parte degli interessati e se il processo è conforme al RGPD (Art. 7 e 8 del GDPR)

Diritto di accesso e alla portabilità

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?Descrivere, in che modo gli interessati possono esercitare i loro diritti di accesso e portabilità dei dati, in conformità agli artt. 15 e 20 GDPR. Se il trattamento beneficia di esenzioni specificate dal diritto di accesso e dal diritto alla portabilità, come previsto nel GDPR darne indicazione

Diritto di rettifica e cancellazione

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto oblio)? descrizione delle misure per garantire agli interessati i diritti di rettifica e cancellazione dei dati: identificare o determinare, anche in riferimento ai valori presenti nella tabella, in che modalità gli interessati possono esercitare i loro diritti di rettifica e cancellazione (diritto all'oblio) (Art. 16 e 17 GDPR), salve eventuali esenzioni dal diritto di rettifica e cancellazione, come previsto negli articoli 16 e 17 del GDPR

Diritto di limitazione e di opposizione

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?descrizione delle misure per garantire agli interessati i diritti di limitazione e opposizione: identificare o determinare in che modalità gli interessati possono esercitare i loro diritti di limitazione e opposizione ai sensi dell'art. 18 e 21 del GDPR). Salve eventuali esenzioni

Responsabile del trattamento esterno

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto? Determinazione e descrizione delle misure applicabili agli obblighi del responsabile del trattamento: identificare o determinare, in riferimento ai valori presenti nella tabella, in che modalità gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto (Art. 28 del GDPR)

Nome del responsabile del trattamento esterno (se già individuato)	Finalità del trattamento	Ambito di applicazione, caratteristiche e garanzie del responsabile	Riferimenti relativi al contratto (se già sottoscritto)	Conformità con l'Articolo 28 del GDPR

Trasferimento dei dati

In caso di trasferimento dei dati al di fuori dell'unione Europea, i dati godono di una protezione equivalente? descrivere le misure applicabili ai dati da trasferire al di fuori dell'Unione Europea: identificare o determinare, in riferimento ai valori presenti nella tabella, in che modalità i dati trasferiti all'esterno dell'Unione Europea godono comunque di una protezione adeguata (Art. 44-49 del GDPR). Specificare il luogo di conservazione delle varie tipologie di dati oggetto di trattamento. A seconda del Paese in questione, si deve giustificare la scelta di conservare i dati al di fuori dell'UE e indicare le salvaguardie legali implementate al fine di garantire un'adeguata protezione dei dati oggetto di trasferimento oltre frontiera

Tipologia di dati e luogo di conservazione	Italia	Unione europea	Stati riconosciuti come adeguati nella protezione dei dati dall'Unione Europea / Verso gli Stati Uniti a una società che ha aderito al Privacy Shield	Altri stati	Giustificazione e supervisione (standard contrattuali, clausole o regolamenti interni)

3.3 Valutazione e modalità di gestione dei rischi dei soggetti interessati

La valutazione e modalità di gestione dei rischi costituisce un aspetto fondamentale degli obblighi dei Delegati del Titolare. Il rischio inerente al trattamento dei dati personali è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (rif. "Considerando" 75-77 del GDPR). Tali impatti dovranno essere, analizzati attraverso un apposito processo di valutazione (Art. 35-36 GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative che il Delegato del Titolare ritiene di dover adottare per mitigare tali rischi

Si riportano di seguito i risultati dell'attivita di valutazione e gestione dei rischi dei soggetti interessati, condotta sul trattamento in esame. **Per ogni ulteriore dettaglio si rimanda al documento in allegato "Analisi dettagliata dei rischi degli interessati" (Tool[2] ARIEC, formato MS Excel)**, tramite la procedura ARIEC descritta nel documento "D04_SCO.1_FASE1 - Metodologia della valutazione d'impatto per la protezione dei dati personali (DPIA)".

3.3.1 Identificazione delle possibili minacce di violazione dei dati personali

Si riportano di seguito, evidenziandole con "X" nella colonna "Selezione", le minacce identificate per il trattamento in esame.

Tipologie	Minacce	Selezione*
1. Eventuale DISTRUZIONE* non autorizzata di dati personali, trattati dal titolare, di lunga durata o irreversibile * Questo tipo di violazione non esclude comunque la possibilità di recuperare in tutto o in parte i dati personali: a) contattando direttamente l'Interessato; b) accedendo a fonti esterne, quali fonti pubbliche e/o di terze parti (es: Pubbliche Amministrazioni); c) accedendo ad archivi cartacei (in caso di distruzione, il recupero da tali archivi si suppone comunque estremamente complesso, di lunga durata e con il rischio di ottenere dati non aggiornati).	1.1 Eliminazione logica non autorizzata di dati personali (es. cancellazione dei dati)	
	1.2 Eliminazione fisica di supporti contenenti dati personali (es. danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei)	
	1.3 Eliminazione logica o del supporto fisico dell'unica copia elettronica di dati personali, il cui ripristino da documenti cartacei è possibile, ma richiede un tale impiego di tempo da poter generare effetti sull'Interessato	
2. Eventuale INDISPONIBILITÀ* di mezzi e strumenti, necessari per il trattamento, temporanea o irreversibile** * L'Indisponibilità riguarda i mezzi e gli strumenti necessari per effettuare i trattamenti da parte degli interessati (per gestire i suoi dati) o da parte del Titolare, per l'erogazione di servizi richiesti o per conto dell'Interessato. L'Indisponibilità non implica la Distruzione. ** L'Indisponibilità irreversibile di un mezzo o strumento richiede l'adozione di nuovi mezzi o strumenti per accedere ai dati.	2.1 Indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (es. in caso di attacco informatico)	
	2.2 Indisponibilità dei mezzi e degli strumenti necessari per ottenere l'accesso alle informazioni (es. perdita di una chiave di decifratura o di un token hardware per accedere a dati in backup o altri archivi)	
	2.3 Indisponibilità degli strumenti atti a identificare l'informazione all'interno di grandi archivi cartacei o elettronici	
	2.4 Degrado prestazionale dei servizi informatici, che determina l'impossibilità di perfezionare operazioni di trattamento	

[2] Per ogni approfondimento metodologico sulla procedura di analisi dei rischi utilizzata, si rimanda anche al documento "D04_SCO.1_FASE1 - Metodologia della valutazione d'impatto per la protezione dei dati personali (DPIA)"

Tipologie	Minacce	Selezione*
	2.5 Modifiche tecnologiche che rendono impossibile la decodifica di dati rappresentati secondo particolari formati di memorizzazione	
3. Eventuale PERDITA* di supporti di memorizzazione di dati personali * La Perdita di un supporto fisico di memorizzazione dei dati non implica che si verifichino anche altre violazioni quali Distruzione, Indisponibilità, Accesso o Divulgazione: ad esempio, un disco DVD perso può contenere una copia cifrata di dati.	3.1 Privazione o sottrazione di supporti fisici di memorizzazione dei dati	
	3.2 Smarrimento di supporti fisici di memorizzazione dei dati	
4. Eventuale ALTERAZIONE* non autorizzata di dati personali * L'Alterazione può essere conseguente, in alcuni casi, ad Accesso non autorizzato, o può essere dovuta, in altri casi, ad errori nel trattamento.	4.1 Comunicazione di informazioni erronee a enti esterni all'azienda (es. istituzioni, società, persone, ecc..) o al pubblico (Internet), determinata da alterazioni non autorizzate di dati personali	
	4.2 Errori nel trattamento o trattamento non conforme, determinati da alterazioni non autorizzate di dati personali	
	4.3 Decisioni errate con effetti sull'Interessato, determinate da alterazioni non autorizzate di dati personali	
5. Eventuale DIVULGAZIONE* non autorizzata di dati personali (non già pubblici) * La Divulgazione può essere conseguente, in alcuni casi, ad Accesso non autorizzato, o può essere dovuta, in altri casi, a trattamenti non conformi di dati riservati.	5.1 Comunicazione non autorizzata od impropria di dati personali, non corrispondenti a informazioni di pubblico dominio, verso terze parti, anche se note o non identificabili.	
	5.2 Diffusione non autorizzata od impropria di dati personali, non corrispondenti a informazioni di pubblico dominio	
6. Eventuale ACCESSO* non autorizzato a dati personali * L'Accesso non autorizzato non implica automaticamente anche la Distruzione, l'Alterazione o la Divulgazione. Il soggetto non autorizzato potrebbe utilizzare a proprio favore le informazioni ricavabili dall'accesso ai dati senza distruggerli, alterarli o divulgarli.	6.1 Accesso effettivo a dati personali (anche in sola visualizzazione) da parte di soggetti non autorizzati al momento della violazione	

*** Legenda delle valutazioni inserite:**

- X - Minaccia selezionata
- <vuoto> - Minaccia non selezionata

3.3.2 Stima del livello di impatto sugli interessati

Si riporta di seguito il livello di impatto sugli interessati, conseguente ai possibili incidenti di sicurezza sui dati personali.

Possibile incidente di sicurezza sui dati personali	Conseguente livello di impatto sugli interessati*
Perdita della disponibilità dei dati personali	

Perdita dell'integrità dei dati personali	
Perdita della riservatezza dei dati personali	
STIMA DEL LIVELLO GENERALE DI IMPATTO	

*** Legenda delle valutazioni inserite:**

- Basso - Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema
- Medio - Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà
- Alto - Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà
- Molto Alto - Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare
- N.A. - Non Applicabile

3.3.3 Stima della probabilità di accadimento delle minacce

Si riporta di seguito la probabilità di accadimento delle minacce identificate, in corrispondenza delle diverse aree di rischio definite.

Area di rischio	Probabilità di accadimento delle minacce*
Tecnico - Minacce correlate a risorse di rete e tecniche (hardware e software)	
Organizzativo - Minacce correlate a processi / procedure relativi alle operazioni di trattamento dati	
Operativo - Minacce correlate a parti e persone coinvolte nelle operazione di trattamento	
Statistico - Minacce correlate a settore di operatività e scala del trattamento	
STIMA DELLA PROBABILITÀ GENERALE DI ACCADIMENTO	

*** Legenda delle valutazioni inserite:**

- Bassa - È improbabile che le minacce si materializzino
- Media - C'è una ragionevole possibilità che le minacce si materializzino
- Alta - Le minacce potrebbero materializzarsi

3.3.4 Valutazione del livello di rischio e selezione delle relative misure tecniche e organizzative

Si riporta di seguito il "**livello di rischio inerente**" calcolato per il trattamento in esame.

Livello di rischio inerente	**Inserire il valore***

Si riporta quindi a seguire, la pianificazione delle eventuali **misure di sicurezza da adottare e da consolidare** per la gestione del rischio.

Se non è prevista alcuna misura da adottare, eliminare la tabella seguente e inserire il testo "NON SONO PREVISTE NUOVE MISURE PER LA GESTIONE DEL RISCHIO"

Categoria	**Cod.**	**Misura di sicurezza da ADOTTARE**	**Resp.**	**Pianificazione**
Esempio "Politica generale di sicurezza per la protezione dei dati personali"	Esempio "A.1"	Esempio "L'Ente dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni."	Esempio "Settore X del Dip. Y"	Esempio "Introdurre la politica entro il xx/xx/xxxx"

Se non è prevista alcuna misura da consolidare, eliminare la tabella seguente e inserire il testo "NON SONO PREVISTI INTERVENTI DI CONSOLIDAMENTO DI MISURE ESISTENTI PER LA GESTIONE DEL RISCHIO"

Categoria	**Cod.**	**Misura di sicurezza da CONSOLIDARE**	**Resp.**	**Pianificazione**
Esempio "Politica generale di sicurezza per la protezione dei dati personali"	Esempio "A.1"	Esempio "L'Ente dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni."	Esempio "Settore X del Dip. Y"	Esempio "Aggiornare il capitolo 2 della politica entro il xx/xx/xxxx"

Fare riferimento alla sezione DASHBOARD del documento in allegato "Analisi dettagliata dei rischi degli interessati" (Tool ARIEC, formato MS Excel) per avere una rappresentazione di sintesi di tutti gli interventi previsti.

A seguito della realizzazione di tali interventi, il "**livello di rischio residuo**" finale corrisponderà al livello di rischio Basso (livello prestabilito di accettazione del rischio).

Livello di rischio residuo	**Inserire il valore***

*** Legenda della valutazione inserita:**

- Basso - Livello di rischio inerente basso
- Medio - Livello di rischio inerente medio
- Alto - Livello di rischio inerente alto

3.4 Validazione della DPIA

3.4.1 Parere del Responsabile della protezione dei dati

Si riporta in allegato il parere che il Responsabile della protezione dei dati (RPD) ha espresso in merito al trattamento oggetto di valutazione, a fronte della verifica effettuata sulle informazioni riportate nel presente report e dei risultati emersi dalla valutazione del rischio.

Motivazioni per cui si decida eventualmente di discostarsi dal parere del RPD	

3.4.2 [opzionale] Opinione di soggetti esterni

Si riporta in allegato la relazione sulle opinioni dei soggetti esterni coinvolti mediante consultazione pubblica.

Motivazioni per cui si decida eventualmente di discostarsi dalle opinioni dei soggetti esterni coinvolti	

3.4.3 Decisioni assunte

Di seguito è richiesto di descrivere e motivare tutte le decisioni assunte in merito alla possibilità di:

- *iniziare il trattamento (avendo adottato misure adeguate a mitigare sufficientemente il rischio);*
- *iniziare il trattamento avendo deciso di accettare un rischio superiore alla soglia di accettazione;*
- *interrompere il trattamento e, quindi, non avviare il trattamento.*

3.5 Allegati

Costituiscono parte integrante del presente documento i seguenti allegati:

- Analisi dettagliata dei rischi degli interessati (Tool ARIEC, formato MS Excel)
- Parere del Responsabile della protezione dei dati personali (RPD)
- [opzionale] Relazione sulle opinioni di soggetti esterni coinvolti