Identificativo: D04_SCO.1_FASE1 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

Metodologia di 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

	Nome e Ruolo	Firma
Autore di riferimento		
	Alfredo Mazzitelli (Ntt Data Italia S.p.A.), Referente Servizi Adeguamento Organizzativo - GDPR e MM AgID	
Verifica		
	Gennaro Oriolo (Leonardo S.p.A.), Responsabile Tecnico Erogazione Servizi	
Approvazione		
Autorizzazione		

Lista di Distribuzione

Rev.	Data	Destinatario	Azienda

Registro delle Revisioni

Rev.	Data	Descrizione delle modifiche	Autore di rif.
1.0	23/03/2021	Versione completa	

Calendario degli Incontri Principali

Data	Incontro	Stato
10/02/2020	Approfondimento con Responsabile della Protezione dei Dati su ruoli, responsabilità e attività di gestione della privacy in Regione Calabria	Effettuato
24/02/2020	Intervista GDPR con DIPARTIMENTO ORGANIZZAZIONE, RISORSE UMANE	Effettuato
26/02/2020	Intervista GDPR con DIPARTIMENTO BILANCIO, FINANZE E PATRIMONIO	Effettuato
26/02/2020	Intervista GDPR con STAZIONE UNICA APPALTANTE	Effettuato
27/02/2020	Intervista GDPR con DIPARTIMENTO PRESIDENZA	Effettuato
27/02/2020	Intervista GDPR con DIPARTIMENTO ISTRUZIONE E ATTIVITA' CULTURALI	Effettuato
02/03/2020	Intervista GDPR con DIPARTIMENTO AMBIENTE E TERRITORIO	Effettuato
02/03/2020	Intervista GDPR con DIPARTIMENTO SEGRETARIATO GENERALE	Effettuato
03/03/2020	Intervista GDPR con DIPARTIMENTO INFRASTRUTTURE, LAVORI PUBBLICI E MOBILITA'	Effettuato
30/03/2020	Intervista GDPR con DIPARTIMENTO LAVORO, FORMAZIONE E POLITICHE SOCIALI	Effettuato
02/04/2020	Intervista GDPR con AUTORITA' DI AUDIT	Effettuato
03/04/2020	Intervista GDPR con DIPARTIMENTO TURISMO E SPETTACOLO	Effettuato
08/04/2020	Intervista GDPR con DIPARTIMENTO SVILUPPO ECONOMICO E ATTIVITA' PRODUTTIVE	Effettuato

Data	Incontro	Stato
08/04/2020	Intervista GDPR con DIPARTIMENTO PROGRAMMAZIONE NAZIONALE	Effettuato
09/04/2020	Intervista GDPR con DIPARTIMENTO AGRICOLTURA E RISORSE AGROALIMENTARI	Effettuato
14/04/2020	Intervista GDPR con DIPARTIMENTO TUTELA DELLA SALUTE E POLITICHE SANITARIE	Effettuato
15/04/2020	Intervista GDPR con DIPARTIMENTO PROGRAMMAZIONE COMUNITARIA	Effettuato
20/04/2020	Intervista GDPR con AVVOCATURA REGIONALE	Effettuato
27/04/2020	Intervista GDPR con NUCLEO VALUTAZIONE	Effettuato
08/05/2020	Intervista GDPR con DIPARTIMENTO URBANISTICA E BENI CULTURALI	Effettuato
14/05/2020	Intervista GDPR con ANTICORRUZIONE E TRASPARENZA	Effettuato
16/06/2020	Intervista GDPR con referenti dei Centri per l'Impiego	Effettuato
29/07/2020	Intervista per adeguamenti privacy con team piattaforma Terzo Settore (Progetto RUNTS)	Effettuato
17/09/2020	Intervista per adeguamenti privacy con Direttore Centro per l'Impiego di Cosenza e referenti delle diverse aree	Effettuato
28/10/2020	Intervista per adeguamenti privacy con referente Ufficio Collocamento Mirato di Cosenza	Effettuato
03/12/2020	Stato di avanzamento delle attività di progetto e condivisione dei prossimi passi con Responsabile Ufficio Privacy	Effettuato
22/12/2020	Approfondimento con SETTORE ECONOMATO, LOGISTICA E SERVIZI TECNICI su necessità DPIA per Sistema Videosorveglianza dell'ente	Effettuato

SOMMARIO

LISTA DELLE TABELLE

LISTA DELLE FIGURE

1 INTRODUZIONE

Il presente deliverable ha l'obiettivo di fornire all'Ente, nelle figure preposte, una metodologia chiara ed esaustiva che li supporti nella gestione delle attività volte ad adempiere l'obbligo descritto negli artt. 35 e 36 del regolamento GDPR, ovvero gli aspetti relativi al Data Protection Impact Assessment
I Titolari del trattamento sia pubblici che privati, e i loro delegati, sono obbligati ad applicare quanto previsto dal regolamento negli articoli suddetti; la valutazione di impatto sulla protezione dei dati prevede la descrizione del trattamento e la valutazione della necessità e proporzionalità, l'analisi dei rischi delle persone interessate, derivanti dal trattamento dei loro dati, e l'individuazione delle misure necessarie per mitigarli.

La DPIA è pertanto uno strumento di riferimento per l'accountability dei Titolari, in quanto consente di dimostrare la consapevolezza dei rischi e gli interventi messi in campo per adempiere agli obblighi del GDPR.

2 RIFERIMENTI

2.1 Documenti Applicabili

Rif.	Codice	Titolo
DA-1.	PRO_ITAL_170635 Rev. 4.1	Progetto dei fabbisogni
DA-2.	CIG 8025774638	Contratto Esecutivo del 05/12/2019

Tabella 1 Documenti applicabili

2.2 Documenti di Riferimento

Rif.	Codice	Titolo
DR-1.	REP_DPIA	Documentazione su valutazioni di impatto sulla protezione dei dati fornita da Dipartimenti, Strutture equiparate e uffici di diretta collaborazione di Regione Calabria, nel periodo febbraio 2020 – marzo 2021.
DR-2.	WP248	Linee guida dello European Data Protection Board in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679.
DR-3.	ISO27001	Standard ISO/IEC 27001:2013 sui Sistemi di Gestione della Sicurezza delle Informazioni.
DR-4.	MAN_ENISA	Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali.
DR-5.	LG_POLIMI	Linea Guida, dell'Osservatorio Information Security & Privacy del Politecnico di Milano, per la Data Protection Impact Assessment.
DR-6.	WP250	Linee guida dello European Data Protection Board in materia di notifica delle violazioni di dati personali (data breach notification)

Tabella 2 Documenti di riferimento

3 DEFINIZIONI E ACRONIMI

3.1 Definizioni

Termine	Descrizione
Anonimizzazione	Tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.
Accountability	Ex art. 5, paragrafo 2 del GDPR: "Il Delegato del Titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Il paragrafo 1 dell'art. 5 del GDPR riguarda i principi fondamentali che devono essere accuratamente applicati ai trattamenti di dati personali
DPIA	Acronimo di Data Protection Impact Assessment (Valutazione di impatto sulla protezione dei dati).
Larga scala	Una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale che potrebbero incidere su un vasto numero di interessati
Misure di sicurezza	Misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.
Pseudonimizzazione	Il 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;

Tabella 3 Definizioni

3.2 Acronimi

Termine	Descrizione
GDPR	General Data Protection Regulation
RPD / DPO	Responsabile della Protezione dei Dati Personali / Data Protection Officer

Tabella 4 Acronimi

4 AMBITO DI APPLICAZIONE

Il nuovo regolamento europeo sulla protezione dei dati personali richiede, all'art.35, l'esecuzione di un Data Protection Impact Assessment (DPIA, a volte indicata anche come PIA) sui dati delle persone fisiche trattati dall'azienda. È in particolare obbligatorio effettuarla quando il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
La valutazione di impatto sulla protezione dei dati è un'attività impiegata per descrivere un trattamento (o un insieme di trattamenti) di dati personali, per valutarne la necessità e la proporzionalità rispetto agli scopi e per determinare le misure necessarie a indirizzare i rischi per i diritti e le libertà delle persone fisiche, valutati in un'analisi preventiva. In tal senso, la DPIA è un modo strutturato ed efficace per rispondere agli obblighi normativi e ha lo scopo di:

- realizzare soluzioni nel rispetto delle prescrizioni del Regolamento in quanto è strumento di ausilio nel processo decisionale circa le misure relative al trattamento;
- dimostrare l'adozione di misure idonee per garantire la conformità alle prescrizioni del Regolamento.

Dunque, la DPIA è uno strumento rilevante per il principio di "accountability" in quanto aiuta il Delegato del Titolare a dimostrare, mediante procedure interne, schemi di analisi, misure tecniche e organizzative, valutazioni quantitative, parametriche o statistiche, evidenze di monitoraggio di indicatori, revisione dei criteri e dei risultati ottenuti, la effettiva protezione dei dati e, in definitiva, la conformità al Regolamento.
Il GDPR stabilisce le caratteristiche minime di una DPIA:

- descrizione delle operazioni di trattamento previste e delle finalità del trattamento;
- una valutazione della necessità e della proporzionalità del trattamento;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per:
    - indirizzare i rischi;
    - dimostrare la conformità al regolamento.

4.1 Norme e best practice di riferimento

- Regolamento (UE) 2016/679, in particolare gli artt. 35 "Valutazione d'impatto sulla protezione dei dati" e 36 "Consultazione preventiva"
- Linee guida dello European Data Protection Board in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 - WP248
- Standard ISO/IEC 27001:2013 sui Sistemi di Gestione della Sicurezza delle Informazioni
- Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali
- Linea Guida, dell'Osservatorio Information Security & Privacy del Politecnico di Milano, per la Data Protection Impact Assessment
- Linee guida dello European Data Protection Board in materia di notifica delle violazioni di dati personali (data breach notification) - WP250

4.2 Violazioni e sanzioni

Con il termine violazioni si fa riferimento a quelle irregolarità nella gestione della DPIA che possono essere oggetto di sanzione a seguito di accertamenti delle Autorità di Controllo. A titolo di esempio si può fare riferimento alla mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa, l'esecuzione in maniera errata di detta valutazione oppure la mancata consultazione dell'Autorità di Controllo laddove richiesto. La violazione di una di queste disposizioni può comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di euro oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

5 METODOLOGIA DI DPIA

La metodologia introdotta con il presente documento si articola in cinque fasi operative organizzate al loro interno in eventuali step e sotto-fasi.

- **Fase A. Pre-valutazione della necessità di DPIA**
  - Step 1. Esame dei casi ex art. 35, par. 3 del GDPR
  - Step 2. Esame delle tipologie ex provv. n. 467, 11 ottobre 2018 del Garante
  - Step 3. Esame dei criteri introdotti dalle linee guida WP248
  - Step 4. Valutazione conclusiva

- **Fase B. Convocazione del Team DPIA**

- **Fase C. Analisi dei rischi degli interessati**
  - Fase 1. Raccolta di informazioni sul trattamento
  - Fase 2. Identificazione delle minacce e dei relativi incidenti di sicurezza sui dati personali
  - Fase 3. Stima del livello di impatto sugli interessati
  - Fase 4. Stima della probabilità di accadimento delle minacce
  - Fase 5. Valutazione del livello di rischio e selezione delle misure di sicurezza appropriate (trattamento del rischio)

- **Fase D. Formalizzazione delle risultanze e consultazione preventiva**

- **Fase E. Riesame della DPIA**

5.1 Fase A. Pre-valutazione della necessità di DPIA

Il primo obiettivo dell'attività, a cura del Delegato del Titolare e con l'eventuale coinvolgimento del Settore Referente Privacy Regionale, riguarda la decisione circa l'opportunità di eseguire la DPIA su un trattamento di propria competenza. Tale decisione è supportata da una rapida valutazione del rischio potenziale che il trattamento potrebbe avere nei confronti dei soggetti interessati. **Per tutti gli scenari potenziali di rischio non trascurabile sarà necessario procedere con la DPIA**.

La prima fase della metodologia supporta il Delegato del Titolare in questa decisione, attraverso quattro step di valutazione del trattamento da eseguire in sequenza. In ogni step dovrà essere valutata in particolare l'eventuale correlazione del trattamento con i relativi scenari indicati, facendo riferimento alle informazioni generali disponibili.

- Step 1. Esame dei casi dell'art. 35, par. 3 del GDPR, per cui la DPIA è NECESSARIA
- Step 2. Esame delle tipologie di trattamento previste dal provvedimento n. 467, 11 ottobre 2018 del Garante per la protezione dei dati personali, per cui la DPIA è NECESSARIA
- Step 3. Esame dei criteri introdotti dalle linee guida WP248, per cui la DPIA è RACCOMANDATA
- Step 4. Valutazione conclusiva

5.1.1 Step 1. Esame dei casi ex art. 35, par. 3 del GDPR

Il Delegato del Titolare dovrà valutare se il trattamento è riconducibile ad uno dei casi sotto indicati. Se il trattamento rientra in almeno uno di essi, la conduzione della DPIA è allora NECESSARIA, ai sensi dell'art. 35, par. 3 del GDPR, e si passerà alla valutazione conclusiva (Step 4). Se il trattamento non rientra in nessuno di essi si passerà allo step successivo (Step 2).

Trattamenti ex art. 35, par. 3 del GDPR	Correlazione
1.1 Il trattamento riguarda una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche?	
1.2 Il trattamento è effettuato su larga scala e riguarda categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR?	
1.3 Il trattamento riguarda la sorveglianza sistematica su larga scala di una zona accessibile al pubblico?	

Tabella 5 Definizione della necessità di realizzazione della DPIA (ex art. 35, par. 3 del GDPR)

5.1.2 Step 2. Esame delle tipologie ex provv. n. 467, 11 ottobre 2018 del Garante

Il Delegato del Titolare dovrà valutare se il trattamento è riconducibile a una delle tipologie sotto indicate. Se il trattamento rientra in almeno una di esse[1], la conduzione della DPIA è allora necessaria, ai sensi del provvedimento n. 467 dell'11 ottobre 2018 del Garante per la protezione de dati personali, e si passerà alla valutazione conclusiva (Step 4).

Trattamenti ex provv. n. 467, 11 ottobre 2018 del Garante	Correlazione
2.1 Il trattamento riguarda attività valutative o di scoring su larga scala, nonché attività che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato (Considerando 71 e 91 RGPD)"?	
2.2 Il trattamento riguarda attività automatizzate finalizzate ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)?	
2.3 Il trattamento prevede un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché la gestione di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati? Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.	
2.4 Il trattamento è effettuato su larga scala e riguarda dati aventi carattere estremamente personale (v. WP248, rev. 01)? Si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	

[1] Nel caso in cui sia stata individuata solo la tipologia 2.7, si passerà comunque allo step successivo (Step 3) per valutare l'applicazione di almeno 1 criterio delle linee guida WP 248.

Trattamenti ex provv. n. 467, 11 ottobre 2018 del Garante	Correlazione
2.5 Il trattamento è effettuato nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP248, rev. 01, in relazione ai criteri nn. 3, 7 e 8)?	
2.6 Il trattamento riguarda attività non occasionali su dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)?	
2.7 Il trattamento è effettuato attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking)?	
2.8 Il trattamento comporta lo scambio tra diversi titolari di dati su larga scala con modalità telematiche?	
2.9 Il trattamento di dati personali è effettuato mediante interconnessione, combinazione o raffronto di informazioni, comprese attività che prevedono l'incrocio dei dati di consumo di beni digitali, con dati di pagamento (es. mobile payment)?	
2.10 Il trattamento riguarda categorie particolari di dati ai sensi dell'art. 9 del GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 del GDPR interconnessi con altri dati personali raccolti per finalità diverse?	
2.11 Il trattamento riguarda attività sistematiche su dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, oppure della persistenza, dell'attività di trattamento?	
2.12 Il trattamento riguarda attività sistematiche su dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, oppure della persistenza, dell'attività di trattamento?	

Tabella 6 Definizione della necessità di realizzazione della DPIA (ex provvedimento Garante)

L'elenco di cui sopra può essere modificato dall'Autorità di Controllo per cui è necessario verificarne preliminarmente l'aggiornamento sul sito istituzionale del Garante per la protezione dei dati personali.

5.1.3 Step 3. Esame dei criteri introdotti dalle linee guida WP248

Il Delegato del Titolare dovrà valutare se il trattamento soddisfa i criteri sotto indicati. Se il trattamento soddisfa almeno due[2] di essi, la conduzione della DPIA è allora RACCOMANDATA, in base alle linee guida WP248, e si passerà alla valutazione conclusiva (Step 4). Se il trattamento non soddisfa nessuno di essi si passerà comunque alla valutazione conclusiva.

Criteri[3] introdotti dalle linee guida WP248	Correlazione
3.1 Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione	
3.2 Processo decisionale automatizzato che ha effetti giuridici o incida in modo analogo significativamente sui diritti degli interessati	
3.3 Monitoraggio sistematico, utilizzato per osservare, monitorare o controllare gli interessati	

[2] Nel caso in cui era stata, al precedente Step 2, individuata la tipologia 2.7, sarà sufficiente soddisfare almeno 1 criterio (invece che 2) per raccomandare la conduzione della DPIA.

[3] Note sui criteri riportati in tabella:

- 3.1. In particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato");
- 3.3. Ivi inclusi, ad es., i dati raccolti tramite reti (es., internet) o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"; il concetto di "sistematico" va inteso secondo uno più dei seguenti criteri: - effettuato secondo un sistema; preorganizzato, organizzato o metodico; effettuato nell'ambito di un piano generale per la raccolta dei dati; - svolto come parte di una strategia;
- 3.4. Trattamenti che mirano a consentire, modificare o rifiutare l'esercizio di un diritto degli interessati ovvero l'accesso degli interessati a un servizio oppure la stipula di un contratto (ad es., screening dei clienti di una banca attraverso i dati della Centrale Rischi al fine di stabilire se ammetterli o meno al finanziamento);
- 3.5. Ad esempio, nel caso di interconnessione di banche dati: a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
- 3.6. Ad es., combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, Internet of Things, etc.;
- 3.7. Indirizzo IP, email, agende digitali…); dati finanziari (situazione economica o patrimoniale, rischio solvibilità, etc.);
- 3.8. In proposito, le linee guida WP 29 consigliano i seguenti criteri per determinare se il trattamento sia svolto su larga scala: - numero di soggetti interessati, sia come numero specifico che come percentuale rispetto all'universo di interessati di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati; - durata o persistenza dell'attività di trattamento; - estensione geografica del trattamento;
- 3.9. Ovvero tutte quelle categorie di persone che potrebbero essere coartate nelle proprie volontà a causa dello squilibrio di potere tra gli stessi e il titolare del trattamento (es., minori, dipendenti, infermi di mente, richiedenti asilo o anziani, pazienti…).

Criteri[3] introdotti dalle linee guida WP248	Correlazione
3.4 Impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	
3.5 Creazione di corrispondenze o combinazione/raffronto di insiemi di dati	
3.6 Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative	
3.7 Dati sensibili o dati aventi carattere altamente personale	
3.8 Trattamento di dati su larga scala (a livello regionale, nazionale o sovranazionale)	
3.9 Dati relativi a interessati vulnerabili[8]	

Tabella 7 Definizione della necessità di realizzazione della DPIA (ex linee guida WP248)

5.1.4 Step 4. Valutazione conclusiva

Qualsiasi sia l'esito della valutazione effettuata negli step precedenti, si ricorda comunque che la conduzione della DPIA non è richiesta nei seguenti casi specifici:

a) quando il trattamento rientri in una delle casistiche di esclusione espressamente definite dall'Autorità Garante nazionale e dal Comitato dei Garanti europei;
b) quando il trattamento non è tale da presentare un «rischio elevato»;
c) quando il trattamento è del tutto simile ad altri per i quali sia già stata effettuata una DPIA;
d) quando il trattamento sia obbligatorio per legge (nazionale o comunitaria), avendo quindi una base giuridica rinvenibile in un obbligo legale (art. 6, par. 1, lett. d del GDPR) o in un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare (art. 6, par. 1, lett. e del GDPR), ma sempre che:
    - la normativa disciplini il trattamento specifico o l'insieme di trattamenti in questione e
    - sia già stata effettuata una DPIA nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica.

In considerazione delle valutazioni effettuate, dei casi di esclusione riportati e di ulteriori informazioni acquisite sul trattamento, il Delegato del Titolare stabilisce se procedere o meno con la DPIA, convocando di conseguenza, in caso affermativo, il Team DPIA.

5.2 Fase B. Convocazione del Team DPIA

Nel caso in cui nella fase precedente è emersa la necessità di effettuare una DPIA, il Delegato del Titolare stabilisce la strategia di DPIA e provvede a convocare il team che si occuperà, in particolare, delle attività di valutazione e trattamento dei rischi dei soggetti interessati al trattamento.

Tale Team DPIA dovrà essere costituito da:

- il **Delegato del Titolare del trattamento**, che coordina le attività;
- uno o più **funzionari competenti del trattamento** oggetto di DPIA, appartenenti alla struttura del Delegato del Titolare e ad altre strutture interne eventualmente coinvolte nel trattamento;
- un referente del **Settore Referente Privacy Regionale**;
- un referente del **Settore Referente Sicurezza Informatica Regionale**;
- il **Responsabile della Protezione dei Dati Personali**;
- gli eventuali **Responsabili di Trattamenti Esterni** (ove presenti) o loro delegati;
- eventuali **consulenti tecnici o giuridici** (qualora necessari).

Di seguito un dettaglio delle responsabilità principali per i componenti necessari del Team DPIA.

Ruoli	Responsabilità principali
Delegato del Titolare del trattamento	• Coordina le attività necessarie alla DPIA per i nuovi trattamenti ed è responsabile della verifica della implementazione delle misure di sicurezza necessarie. • È responsabile della raccolta delle informazioni sul trattamento per le verifiche preventive • È responsabile delle verifiche preventive di conformità del trattamento • Coadiuva il RPD nelle verifiche preventive sull'obbligatorietà della esecuzione di una DPIA • In caso di un trattamento esistente che presenta un cambiamento del profilo di rischio coordina le attività per l'aggiornamento della DPIA • Implementa la strategia nella gestione del trattamento • Partecipa alla valorizzazione degli impatti e probabilità per le minacce individuate • Assiste il RPD nella richiesta di Consultazione Preventiva
Funzionario competente del trattamento oggetto di DPIA	• Descrive e documenta il trattamento in tutte le sue caratteristiche • Collabora con il Delegato del Titolare nella valutazione dell'impatto privacy • Assiste il Delegato del Titolare e il RPD nelle verifiche preventive (conformità e necessità DPIA) • Assiste il Delegato del Titolare nel garantire il rispetto degli obblighi di DPIA, tenendo conto della natura del trattamento e delle informazioni a loro disposizione. • Nel caso in cui il trattamento preveda l'impiego di Sistemi Informatici esterni, si confronta con i Responsabili Esterni che forniscono il servizio. • Supervisiona l'implementazione delle misure di sicurezza necessarie. • Partecipa alla valorizzazione degli impatti e probabilità per le minacce individuate • Collabora con il Delegato del Titolare nelle attività di Consultazione Preventiva.
Settore Referente Privacy Regionale	• Supporta i delegati nelle attività di DPIA
Settore Referente per la Sicurezza Informatica Regionale	• Collabora con il Settore Referente Privacy Regionale nelle attività di definizione e verifica delle misure di sicurezza informatica e nella attività di valutazione di impatto delle attività di trattamento (DPIA)
Responsabile della Protezione dei Dati Personali	• Assiste il Delegato del Titolare nella definizione della Strategia e nello svolgimento della DPIA, monitora lo svolgimento, verifica se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR. • È responsabile della verifica preventiva di obbligatorietà della DPIA • Coadiuva il Delegato del Titolare nella verifica preventiva di conformità del trattamento • È responsabile delle attività di consultazione preventiva e funge da interfaccia per l'Autorità di Controllo.

Tabella 8 Ruoli e responsabilità nel Team DPIA

Lavorare in team permette di effettuare una valutazione che è tanto più efficace quanto più coinvolga soggetti provenienti anche da ambiti diversi da quello del trattamento in esame, per evidenziare rischi da più punti di vista e soluzioni già note e/o applicate.

5.2.1 Matrice RACI

Si rappresenta di seguito, nel formalismo della matrice RACI, l'attribuzione di responsabilità per le principali attività di DPIA, in riferimento alle fasi della metodologia in cui sono eseguite. Si evidenzia, inoltre, con un colore differente, l'attività "Pre-valutazione necessità DPIA", in quanto eseguita al di fuori del Team DPIA.

RUOLI / ATTIVITÀ PRINCIPALI	Pre-valutazione necessità DPIA [cfr. Fase A]	Definizione strategia DPIA e convocazione Team DPIA [cfr. Fase B]	Approfondimento informazioni trattamento [cfr. Fase C/1]	Valutazione rischi soggetti interessati [cfr. Fase C/2-4]	Selezione misure sicurezza per trattamento rischi [cfr. Fase C/5]	Redazione Report DPIA da inoltrare a DPO [cfr. Fase D]	Formulazione parere DPO [cfr. Fase D]	Approvazione Report DPIA [cfr. Fase D]	Consultazione preventiva Garante [cfr. Fase D]	Riesame DPIA [cfr. Fase E]
Delegato del Titolare per il trattamento oggetto di DPIA	A	A	A	A	A	A		A	A/R	A
Funzionario competente del trattamento oggetto di DPIA	R	R	R	R	R	R		I		R
Settore Referente Privacy Regionale	C	C	C	C	C	C		I	C	C
Settore Referente per la Sicurezza Informatica Regionale		C	C	C	C	C		I		C
Responsabile della Protezione dei Dati Personali		C		C	C		A/R	I	C	C
Responsabile del Trattamento Esterno o suo delegato		I	C	C	C	C		I	I	C

Figura 1 Matrice RACI per attività di DPIA

Legenda:

- Responsible (R): esegue e/o assegna l'attività;
- Accountable (A): ha la responsabilità sul risultato dell'attività (univocamente assegnato);
- Consulted (C) collabora nell'esecuzione dell'attività;
- Informed (I): è informato dell'esecuzione dell'attività.

5.3 Fase C. Analisi dei rischi degli interessati

Una componente centrale della DPIA è rappresentata dall'analisi dei rischi dei soggetti interessati al trattamento. È necessario che l'attività di analisi sia condotta con un approccio ben definito, condiviso e ripetibile in grado di accompagnare l'Ente in un processo ricorrente da ripetersi con cadenza programmata e ad ogni cambiamento del trattamento o del contesto di riferimento.
L'analisi dei rischi è un'attività utile a identificare e valutare i possibili scenari di rischio che mettono a repentaglio le libertà e i diritti fondamentali degli interessati. Tale attività consente inoltre di giustificare le contromisure da adottare, in termini di costi e benefici, valutando la loro efficacia rispetto alle minacce di violazione dei dati personali e ai possibili impatti sugli interessati.

La procedura di analisi dei rischi introdotta nella presente metodologia di DPIA si basa sul security framework di ENISA (Agenzia dell'Unione europea per la cibersicurezza) e sulla modellazione del seguente scenario di rischio:

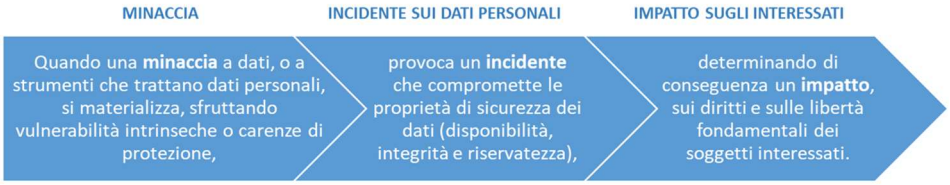


Figura 2 Modellazione scenario di rischio

Le attività si articolano in cinque fasi operative:

- Fase 1. Raccolta di informazioni sul trattamento
- Fase 2. Identificazione delle minacce e dei relativi incidenti di sicurezza sui dati personali
- Fase 3. Stima del livello di impatto sugli interessati
- Fase 4. Stima della probabilità di accadimento delle minacce
- Fase 5. Valutazione del livello di rischio e selezione delle misure di sicurezza appropriate (trattamento del rischio)

5.3.1 Fase 1. Raccolta di informazioni sul trattamento

La prima fase dell'analisi riguarda la raccolta e l'approfondimento di tutte le informazioni sul trattamento:

- la natura, l'ambito, il contesto del trattamento;
- le finalità del trattamento (determinate, esplicite e legittime);
- la base giuridica del trattamento;
- la tipologia dei dati (adeguati, pertinenti e limitati a quanto necessario);
- la tipologia di interessati coinvolti;
- i tempi di conservazione (limitati allo stretto indispensabile);
- l'individuazione degli strumenti utilizzati per il trattamento (hw, sw, reti, etc.)

e delle misure tecniche e organizzative già previste/adottate:

- l'assegnazione delle responsabilità per il trattamento (interne ed esterne al Titolare);
- le garanzie adottate per la minimizzazione, l'esattezza e l'aggiornamento dei dati;
- le modalità di rilascio dell'informativa ed (eventuale) acquisizione del consenso;
- i canali disponibili e le garanzie in merito all'esercizio dei diritti degli interessati;
- le garanzie adottate in caso di trasferimento dei dati in paesi od organizzazioni terze.

In tale fase il Team DPIA dovrà anche verificare che vi siano tutti i presupposti per effettuare un trattamento conforme ai requisiti di legittimità previsti dal GDPR.

In caso affermativo si procederà con le fasi successive, tenendo a disposizione tutte le informazioni raccolte, ma concentrandosi in particolare sugli elementi informativi minimi, riportati nel questionario in figura, per identificare ed esaminare gli scenari di rischio.

1.1. DESCRIVERE IL TRATTAMENTO COMPILANDO TUTTI GLI ELEMENTI INFORMATIVI MINIMI SEGUENTI

Dati personali oggetto di trattamento	Finalità del trattamento	Soggetti interessati
Strumenti impiegati nel trattamento	**Destinatari dei dati**	**Responsabile del trattamento**

Figura 3 Questionario per raccolta elementi informativi minimi sul trattamento

5.3.2 Fase 2. Identificazione delle minacce e dei relativi incidenti di sicurezza sui dati personali

Completata la fase di approfondimento delle caratteristiche del trattamento, si procede con l'identificazione delle possibili minacce di violazione dei dati che sfruttando vulnerabilità o carenze di protezione in essere compromettono le proprietà di sicurezza dei dati.

Si consideri che l'intera attività di DPIA, così come tutte le attività volte a proteggere i trattamenti, hanno come obiettivo principale quello di minimizzare la probabilità e l'impatto che possibili violazioni di dati personali possono comportare sugli individui.

Le principali tipologie di violazioni riguardano la:

1. **DISTRUZIONE** non autorizzata di dati personali, trattati dal titolare, di lunga durata o irreversibile;
2. **INDISPONIBILITÀ** di mezzi e strumenti, necessari per il trattamento, temporanea o irreversibile;
3. **PERDITA** di supporti di memorizzazione di dati personali;
4. **ALTERAZIONE** non autorizzata di dati personali;
5. **DIVULGAZIONE** non autorizzata di dati personali (non già pubblici);
6. **ACCESSO** non autorizzato a dati personali.

La figura seguente schematizza il questionario[4] a risposta multipla che dovrà essere compilato nella presente fase (selezionando semplicemente una o più voci disponibili) per identificare le principali minacce in corrispondenza delle suddette tipologie di violazioni.

[4] Questionario basato su "Linea Guida, dell'Osservatorio Information Security & Privacy del Politecnico di Milano, per la Data Protection Impact Assessment"

2.1. SELEZIONARE LE MINACCE CHE POSSONO RAGIONEVOLMENTE MATERIALIZZARSI SFRUTTANDO VULNERABILITÀ O CARENZE DI PROTEZIONE IN ESSERE

Tipologie	Minacce	R/mult
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	
	2.5 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 gia' 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	

Figura 4 Questionario per identificazione minacce

In riferimento a quanto previsto dagli artt. 32, 33 e 35, e relativi Considerando del GDPR, le conseguenze sul trattamento, generate dalla realizzazione delle minacce, possono essere ricondotte a tre principali incidenti di sicurezza:

- Perdita Della **Disponibilità** Dei Dati Personali (PD) - I dati personali non sono accessibili o utilizzabili quando necessario;
- Perdita Dell'**Integrità** Dei Dati Personali (PI) - I dati personali sono incompleti o non corretti o modificati senza le opportune autorizzazioni;
- Perdita Della **Riservatezza** Dei Dati Personali (PR) - I dati personali sono divulgati a individui, organizzazioni, enti non autorizzati.

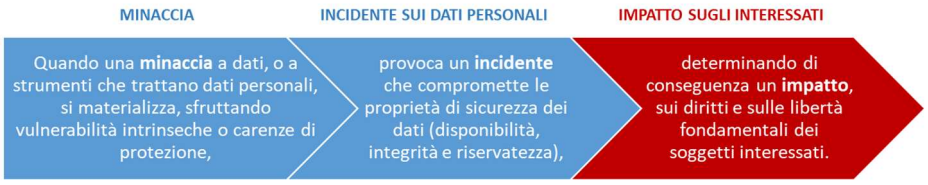
In realtà ogni minaccia può determinare una combinazione dei suddetti incidenti, ma è possibile in generale selezionarne uno quale prevalente, come riportato nella tabella seguente.

Tipologie di minacce	Incidenti di sicurezza
1. DISTRUZIONE	Perdita Della Disponibilità Dei Dati Personali (PD)
2. INDISPONIBILITÀ	Perdita Della Disponibilità Dei Dati Personali (PD)
3. PERDITA	Perdita Della Disponibilità Dei Dati Personali (PD)
4. ALTERAZIONE	Perdita Dell'integrità Dei Dati Personali (PI)
5. DIVULGAZIONE	Perdita Della Riservatezza Dei Dati Personali (PR)
6. ACCESSO	Perdita Della Riservatezza Dei Dati Personali (PR)

Tabella 9 Criterio di correlazione tra tipologie minacce e incidenti sicurezza

5.3.3 Fase 3. Stima del livello di impatto sugli interessati

Completata la fase di identificazione delle minacce e dei relativi incidenti di sicurezza sui dati personali, si procede con la stima del possibile impatto sui diritti e le libertà fondamentali dei soggetti interessati.



La figura seguente schematizza il questionario[5] a risposta singola che dovrà essere compilato (selezionando semplicemente una voce disponibile) per stimare il livello generale di impatto.

3.1. STIMARE IL POSSIBILE IMPATTO SUGLI INTERESSATI DOVUTO ALLA PERDITA DELLA DISPONIBILITÀ DEI DATI PERSONALI

Livello d'impatto	Descrizione	Possibili esempi	R/sing
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema	Tempo trascorso reinserendo informazioni, fastidi, irritazioni, etc.	
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà	Costi aggiuntivi, rifiuto/impossibilità di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.	
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà	Appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.	
Molto Alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare	Incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.	

Figura 5 Questionario per stima impatto su interessato in corrispondenza di incidente di sicurezza specificato

Tale questionario dovrà essere compilato distintamente per ogni possibile incidente di sicurezza identificato nella fase precedente, tra:

- Perdita Della **Disponibilità** Dei Dati Personali (PD);
- Perdita Dell'**Integrità** Dei Dati Personali (PI);
- Perdita Della **Riservatezza** Dei Dati Personali (PR).

Il livello generale di impatto corrisponderà infine al valore più alto dei livelli di impatto stimati per ogni distinto incidente di sicurezza.

[5] Questionario tratto dal "Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali".

La stima dell'impatto è una valutazione qualitativa e il Delegato del Titolare deve considerare una serie di fattori per effettuarla correttamente, quali, in particolare, la tipologia e il volume dei dati personali trattati, la finalità del trattamento, le categorie di interessati. Trattandosi di valutazione qualitativa, il livello stimato dovrebbe essere, per completezza, documentato con le assunzioni effettuate per giungere al risultato.

5.3.4 Fase 4. Stima della probabilità di accadimento delle minacce

Ciascun incidente di sicurezza sui dati personali può essere determinato dalla realizzazione di una o più minacce. Quanto sia possibile che tali minacce possano causare un incidente di sicurezza costituisce la misura di probabilità da stimare nella presente fase.

Le figure seguenti schematizzano i questionari[6] che dovranno essere interamente compilati (specificando semplicemente "sì" o "no" su ogni domanda) per stimare la probabilità di accadimento delle minacce identificate nella Fase 2 e correlate a quattro aree di rischio:

- **Area di rischio tecnico** - Minacce correlate a risorse di rete e tecniche (hardware e software)
- **Area di rischio organizzativo** - Minacce correlate a processi / procedure relativi alle operazioni di trattamento dati
- **Area di rischio operativo** - Minacce correlate a parti e persone coinvolte nelle operazioni di trattamento
- **Area di rischio statistico** - Minacce correlate a settore di operatività e scala del trattamento

4.1. AREA DI RISCHIO TECNICO - VALUTA LE MINACCE CORRELATE A RISORSE DI RETE E TECNICHE (HARDWARE E SOFTWARE)

Domanda	Descrizione	R/compl
1. Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.	
2. E' possibile che venga fornito accesso, tramite Internet, a un sistema interno di trattamento dei dati personali (ad esempio per determinati utenti o gruppi di utenti)?	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.	
3. Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno alla struttura organizzativa?	La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno della struttura organizzativa (che in linea di principio non sono autorizzate a tale accesso).	
4. Le persone non autorizzate possono accedere facilmente all'ambiente fisico di trattamento dei dati?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico).	
5. Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le best practice pertinenti?	Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.	

Figura 6 Questionario per stima probabilità minacce in area rischio tecnico

[6] Questionari tratti dal "Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali" e opportunamente adattati al contesto.

4.2. AREA DI RISCHIO ORGANIZZATIVO - VALUTA LE MINACCE CORRELATE A PROCESSI E PROCEDURE RELATIVI ALLE OPERAZIONI DI TRATTAMENTO DATI

Domanda	Descrizione	R/compl
6. I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.	
7. L'uso consentito della rete, del sistema e delle risorse fisiche all'interno della struttura organizzativa è ambiguo o non chiaramente definito?	Quando l'uso accettabile delle risorse non è chiaramente prescritto, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.	
8. I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno della struttura organizzativa potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.	
9. I dipendenti sono autorizzati a trasferire, archiviare o trattare in altro modo i dati personali al di fuori dei locali della struttura organizzativa?	L'elaborazione di dati personali al di fuori dei locali della struttura organizzativa può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.	
10. Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di log file?	La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali.	

Figura 7 Questionario per stima probabilità minacce in area rischio organizzativo

4.3. AREA DI RISCHIO OPERATIVO - VALUTA LE MINACCE CORRELATE A PARTI E PERSONE COINVOLTE NELLE OPERAZIONI DI TRATTAMENTO

Domanda	Descrizione	R/compl
11. Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	
12. Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?	Quando l'elaborazione viene eseguita da contraenti esterni, la struttura organizzativa può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che la struttura organizzativa selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	
13. Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.	
14. Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	
15. Le persone / parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.	

Figura 8 Questionario per stima probabilità minacce in area rischio operativo

4.4. AREA DI RISCHIO STATISTICO - VALUTA LE MINACCE CORRELATE A SETTORE DI OPERATIVITÀ E SCALA DEL TRATTAMENTO

Domanda	Descrizione	R/compl
16. Si ritiene che il settore di operatività in cui si inserisce il trattamento sia esposto ad attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore di operatività, questa è un'indicazione che la struttura organizzativa probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile nel proprio eventuale analogo settore.	
17. La struttura organizzativa ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	Se la struttura organizzativa è già stato attaccato o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	
18. Hai ricevuto notifiche e / o lamentele riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento dei dati personali) nell'ultimo anno?	Bug di sicurezza / vulnerabilità presenti possono essere sfruttati per eseguire attacchi (cyber o fisici) ad altri sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.	
19. Un'operazione del trattamento riguarda un grande volume di individui e / o dati personali?	Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).	
20. Esistono best practice di sicurezza specifiche, per il settore di attività in cui si inserisce il trattamento, che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le best practice pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.	

Figura 9 Questionario per stima probabilità minacce in area rischio statistico

Definendo, per ogni area di rischio, la probabilità di accadimento delle minacce come:

- Bassa: è improbabile che tali minacce si materializzino;
- Media: c'è una ragionevole possibilità che tali minacce si materializzino;
- Alta: tali minacce potrebbero materializzarsi

la stima raccomandata per la probabilità di accadimento sull'area di rischio sarà valorizzata secondo la seguente tabella:

Numero risposte "sì" su area di rischio	Probabilità di accadimento minacce
0-1	Bassa
2-3	Media
4-5	Alta

Tabella 10 Criterio di correlazione tra risposte su aree rischio e probabilità minacce

Tale stima può essere eventualmente modificata, senza rispettare obbligatoriamente il suddetto criterio, documentando opportunamente tale variazione in corrispondenza dell'area di rischio interessata.
Attribuendo successivamente un punteggio, ad ogni area di rischio, secondo la seguente tabella:

Area di rischio	Probabilità di accadimento minacce	Punteggio area
Area di rischio tecnico	Bassa	1
	Media	2
	Alta	3
Area di rischio organizzativo	Bassa	1
	Media	2
	Alta	3
Area di rischio operativo	Bassa	1
	Media	2
	Alta	3
Area di rischio statistico	Bassa	1
	Media	2
	Alta	3

Tabella 11 Criterio di attribuzione punteggio ad aree rischio

si ottiene infine la stima della probabilità generale di accadimento, applicando il criterio riportato in tabella[7]:

Somma punteggi di ogni area di rischio	Probabilità generale di accadimento minacce
4-5	Bassa
6-8	Media
9-12	Alta

Tabella 12 Criterio di valutazione probabilità generale accadimento minacce

5.3.5 Fase 5. Valutazione del livello di rischio e selezione delle misure di sicurezza appropriate

Completate le stime:

- della probabilità generale di accadimento delle minacce identificate e
- del livello generale di impatto sugli interessati,

si procede con la valutazione del livello di rischio inerente (LRI), applicando il criterio[8] rappresentato in figura con la seguente legenda dei colori:

- verde: livello di rischio basso;
- giallo: livello di rischio medio;
- rosso: livello di rischio alto.

		Livello generale di impatto sugli interessati		
		Basso	**Medio**	**Alto / Molto Alto**
Probabilità generale di accadimento delle minacce identificate	**Bassa**			
	Media			
	Alta			

Tabella 13 Criterio di valutazione livello rischio inerente (LRI)

In considerazione del livello di rischio ottenuto andrà valutata l'eventuale esigenza di adottare nuove misure tecniche e organizzative, o consolidare quelle in essere, per contenere il rischio entro livelli accettabili.

Il manuale ENISA sulla "sicurezza nel trattamento dei dati personali" suggerisce un set[9] di misure di sicurezza efficace, ai fini della mitigazione del rischio, modulabile in funzione del livello di rischio da gestire e organizzato in 20 categorie:

- A) Politica generale di sicurezza per la protezione dei dati personali;
- B) Ruoli e responsabilità;
- C) Politica per il controllo degli accessi;
- D) Gestione delle risorse / asset;
- F) Gestione delle modifiche apportare alle risorse, agli apparati e ai sistemi IT;
- G) Responsabili del trattamento;
- H) Gestione degli incidenti / violazioni di dati personali (personal data breaches);

[7] Criterio tratto dal "Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali".
[8] Criterio tratto dal "Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali".
[9] A seconda del contesto del trattamento, la struttura organizzativa potrebbe estendere tale set di misure con obblighi normativi e requisiti di sicurezza settoriali specifici.

- I) Continuità operativa;
- L) Obblighi di confidenzialità;
- M) Formazione;
- N) Controllo degli accessi e autenticazione;
- O) Generazione di file di log e monitoraggio;
- P) Sicurezza dei server e dei database;
- Q) Sicurezza delle postazioni di lavoro;
- R) Sicurezza della rete e delle comunicazioni elettroniche;
- S) Back-up;
- T) Dispositivi mobili / portatili;
- U) Sicurezza nel ciclo di vita delle applicazioni;
- V) Cancellazione / eliminazione dei dati;
- Z) Sicurezza fisica.

Ogni misura del set ENISA è associata ad uno specifico LRI (Basso, Medio, Alto) e dovrebbe essere applicata in tutti i casi in cui il trattamento riveli un LRI maggiore o uguale a quello della misura stessa. Il set ENISA è stato inoltre opportunamente adattato al contesto in esame e integrato con le informazioni sugli incidenti di sicurezza contrastati, per cui è possibile distinguere:

- Misure efficaci contro la Perdita Della Disponibilità Dei Dati Personali (PD);
- Misure efficaci contro la Perdita Dell'Integrità Dei Dati Personali (PI);
- Misure efficaci contro la Perdita Della Riservatezza Dei Dati Personali (PR).

Il Team DPIA, che dovrà occuparsi della selezione delle misure da adottare e da consolidare, potrà utilizzare anche tali informazioni aggiuntive sugli incidenti di sicurezza (in relazione alle minacce identificate) per operare una selezione più aderente al profilo di rischio rilevato.

Si sottolinea che la corretta applicazione di tutte le misure raccomandate del set ENISA consente in generale di contenere il rischio ad un livello accettabile.

A partire dalla lista di tali misure, raccomandate in funzione del livello di rischio del trattamento (LRI) e dei possibili incidenti di sicurezza (PD, PI e PR)) da contrastare, il Team DPIA dovrà indicare una possibile opzione di intervento per ognuna di esse:

- Misura da adottare;
- Misura da consolidare;
- Misura già adottata[10] - Nessun Intervento;
- Misura non applicabile - Nessun Intervento

e, per le misure da adottare e da consolidare, dovrà individuare anche un responsabile dei relativi interventi pianificare. Il **piano di trattamento dei rischi** concorre, insieme a tutte le altre informazioni raccolte dal Team DPIA, alla formalizzazione delle risultanze dell'attività di DPIA.

Si riportano a seguire, in conclusione, una rappresentazione di esempio del set di misure tecniche e organizzative, disponibile in versione completa nell'Allegato 1; e una visualizzazione di esempio della dashboard per il trattamento del rischio inclusa nel Tool ARIEC (cfr. Allegato 2). La dashboard restituisce una efficace rappresentazione di sintesi delle misure da adottare e da consolidare e una panoramica intuitiva delle più importanti aree di intervento da sviluppare.

[10] Alcune delle misure raccomandate potrebbero naturalmente essere già implementate presso la struttura organizzativa.

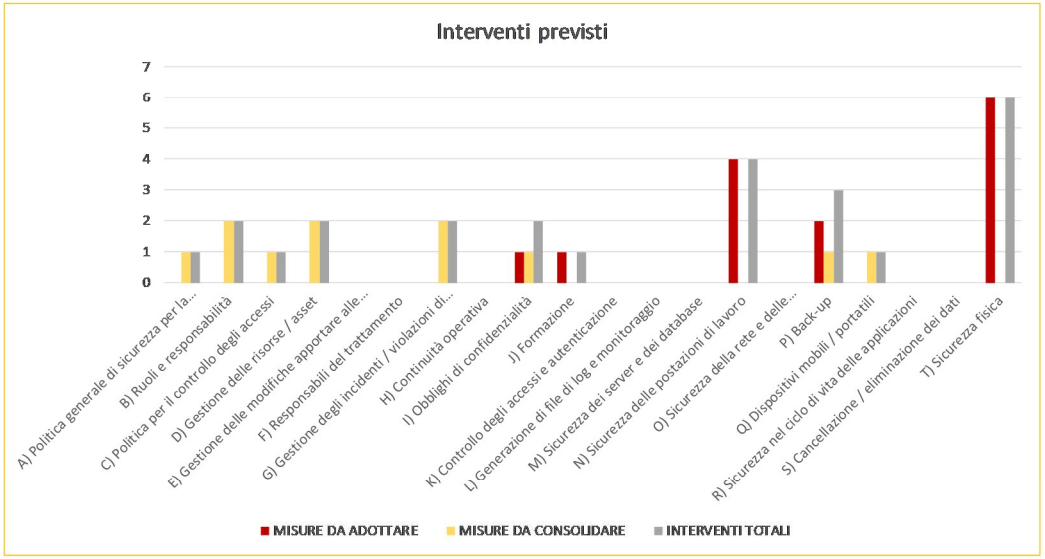
Categoria	Cod.	Misura di sicurezza	Rif. ISO/IEC 27001:2013	LRI	PD	PI	PR	Intervento	Resp.	Pianificazione
N) Sicurezza delle postazioni di lavoro	N.1	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.2	Le applicazioni anti-virus e le firme di rilevamento dovrebbero essere configurate su base settimanale.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.3	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.4	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.5	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo dovrebbero essere installati regolarmente.	14.01 Requisiti di sicurezza dei sistemi informativi	Basso	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.6	Le applicazioni antivirus e le firme di rilevamento dovrebbero essere configurate su base giornaliera.	14.01 Requisiti di sicurezza dei sistemi informativi	Medio	x	x	x			
N) Sicurezza delle postazioni di lavoro	N.7	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	14.01 Requisiti di sicurezza dei sistemi informativi	Alto	x	x	x			

Tabella 14 Rappresentazione di esempio del set di misure[11] tecniche e organizzative

[11] Misure tecniche e organizzative tratte dal "Manuale ENISA (Agenzia dell'Unione europea per la cibersicurezza) sulla Sicurezza nel trattamento dei dati personali", opportunamente adattate al contesto e integrate con informazioni aggiuntive.

DASHBOARD PER IL TRATTAMENTO DEL RISCHIO

AREE DI INTERVENTO	MISURE DA ADOTTARE	MISURE DA CONSOLIDARE	INTERVENTI TOTALI
A) Politica generale di sicurezza per la protezione dei dati personali	0	1	1
B) Ruoli e responsabilità	0	2	2
C) Politica per il controllo degli accessi	0	1	1
D) Gestione delle risorse / asset	0	2	2
E) Gestione delle modifiche apportare alle risorse, agli apparati e ai sistemi IT	0	0	0
F) Responsabili del trattamento	0	0	0
G) Gestione degli incidenti / violazioni di dati personali (personal data breaches)	0	2	2
H) Continuità operativa	0	0	0
I) Obblighi di confidenzialità	1	1	2
J) Formazione	1	0	1
K) Controllo degli accessi e autenticazione	0	0	0
L) Generazione di file di log e monitoraggio	0	0	0
M) Sicurezza dei server e dei database	0	0	0
N) Sicurezza delle postazioni di lavoro	4	0	4
O) Sicurezza della rete e delle comunicazioni elettroniche	0	0	0
P) Back-up	2	1	3
Q) Dispositivi mobili / portatili	0	1	1
R) Sicurezza nel ciclo di vita delle applicazioni	0	0	0
S) Cancellazione / eliminazione dei dati	0	0	0
T) Sicurezza fisica	6	0	6
	14	11	25



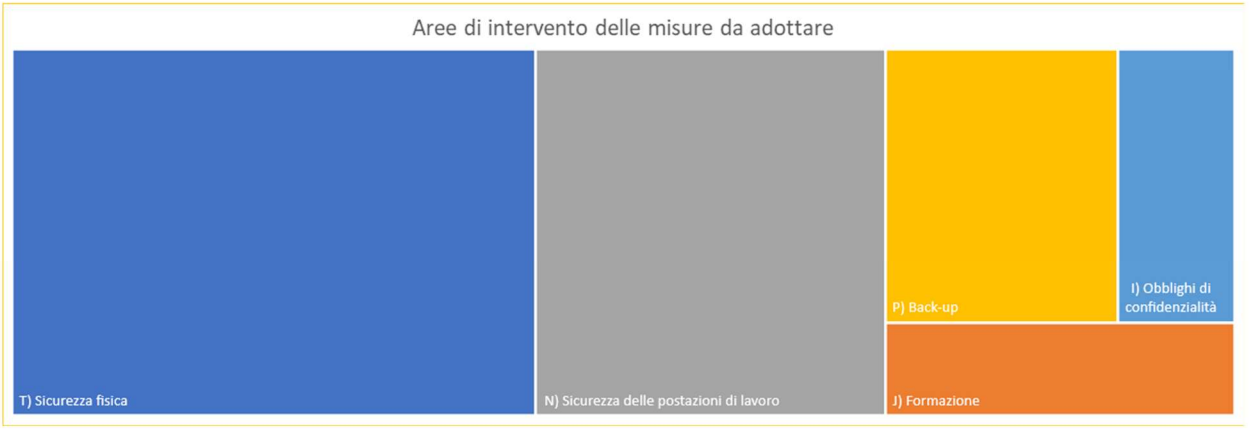


Figura 10 Visualizzazione di esempio della dashboard per il trattamento del rischio inclusa nel Tool ARIEC

5.4 Fase D. Formalizzazione delle risultanze e consultazione preventiva

Tutte le informazioni ottenute nell'ambito della DPIA, dal censimento e descrizione del trattamento, passando dalla valutazione preliminare dell'effettiva necessità di DPIA, per arrivare alla valutazione del rischio e, quando necessario, al relativo piano di trattamento, concorrono alla realizzazione di un **report di sintesi** (cfr. Allegato 3) in grado di rappresentare efficacemente i risultati ottenuti e dimostrare, altresì, la corretta esecuzione formale della stessa attività di DPIA e la sua aderenza ai requisiti richiesti dal GDPR.

È necessario a questo punto, **richiedere ed acquisire il parere finale del RPD** sugli esiti della DPIA. Le linee guida WP248 raccomandano che il parere riguardi almeno:

a) le misure tecniche e organizzative da adottare / da consolidare per mitigare i rischi rilevati;
b) la correttezza nella conduzione della DPIA e la conformità al GDPR delle conclusioni raggiunte circa l'opportunità di procedere con il trattamento.

Inoltre, pur non essendo prevista come obbligatoria, per trattamenti particolarmente complessi, che possono interessare diverse categorie di soggetti esterni, potrebbe essere avviata una **eventuale consultazione pubblica** al fine di acquisire le opinioni di tali categorie di soggetti (ad esempio, enti partner su attività specifiche, cluster di soggetti interessati, etc.).

Ove il Delegato del Titolare si discosti dal parere formalizzato dal RPD e/o dalle opinioni raccolte a seguito dell'eventuale consultazione pubblica, dovrebbe documentare all'interno del report finale le motivazioni alla base della decisione.

Nel caso non sia stato possibile, invece, ottenere un livello accettabile per il rischio residuo, si dovrà obbligatoriamente procedere con la **consultazione preventiva dell'Autorità di Controllo** prima di avviare le attività di trattamento. Più in generale, qualora:

a) la DPIA indichi che il trattamento possa presentare un rischio elevato in assenza di ulteriori misure adottabili dal Delegato del Titolare in grado di attenuare il rischio;
b) si ricada nel campo di applicazione dell'art. 36, par. 5 del GDPR, ovvero il diritto interno preveda comunque la consultazione dell'Autorità di Controllo e/o la sua autorizzazione preliminare, in relazione a trattamenti posti in essere per l'esecuzione di un compito di interesse pubblico,

il Delegato del Titolare dovrà consultare l'Autorità di Controllo, prima di procedere al trattamento. A norma dell'art. 36 del GDPR, all'Autorità di Controllo dovranno essere comunicate le seguenti informazioni:

- l'allocazione delle responsabilità del trattamento;
- le finalità del trattamento;
- i mezzi del trattamento;
- le misure e le garanzie previste;
- gli esiti finali della DPIA effettuata;
- i dati di contatto del RPD;
- ogni altra informazione richiesta dall'Autorità di Controllo.

Il trattamento oggetto di DPIA non potrà essere iniziato a meno che:

- il procedimento di consultazione preventiva si sia concluso con successo;
- non pervenga alcuna risposta dall'Autorità di Controllo entro il termine di otto settimane dal ricevimento della richiesta[12] (silenzio assenso).

[12] Termine eventualmente prorogabile, entro il primo mese dal ricevimento della richiesta, di ulteriori sei settimane sulla base della complessità della trattazione.

5.5 Fase E. Riesame della DPIA

Quando insorgono variazioni del rischio legato alle attività di trattamento, è necessario che il Delegato del Titolare proceda ad un riesame della DPIA per valutare se il trattamento sia ancora effettuato conformemente al nuovo profilo di rischio. Le linee guida WP248 raccomandano di procedere comunque con un riesame, ad intervalli periodici, anche se non dovessero sopraggiungere cambiamenti evidenti del trattamento.

In definitiva:

- si sottolinea la necessità di procedere con il riesame della DPIA in corrispondenza di **variazioni delle condizioni del trattamento** (variazioni processive, tecnologiche, delle misure adottate, etc.) e/o di emersione di **diversi e ulteriori profili di rischio** (eventuali data breach, reiterate richieste di esercizio dei diritti degli interessati, etc.);
- si raccomanda di programmare un riesame periodico della DPIA, con **cadenza almeno annuale** o con periodo tanto minore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nelle attività di trattamento. La frequenza di aggiornamento prevista dovrà essere riportata esplicitamente nel report finale della DPIA.

6 STRUMENTI INFORMATICI A SUPPORTO

La metodologia di DPIA descritta nel presente documento è supportata da due strumenti informatici, il Tool Registri GDPR e il Tool ARIEC (cfr. Allegato 2) che implementano rispettivamente la procedura di pre-valutazione della necessità di DPIA, descritta nella sezione 5.1, e la procedura di analisi dei rischi degli interessati, descritta nella sezione 5.3. Entrambi gli strumenti consentono di semplificare notevolmente due attività centrali e impegnative della metodologia.

Il Tool Registri GDPR è raggiungibile dalla intranet di Regione Calabria.

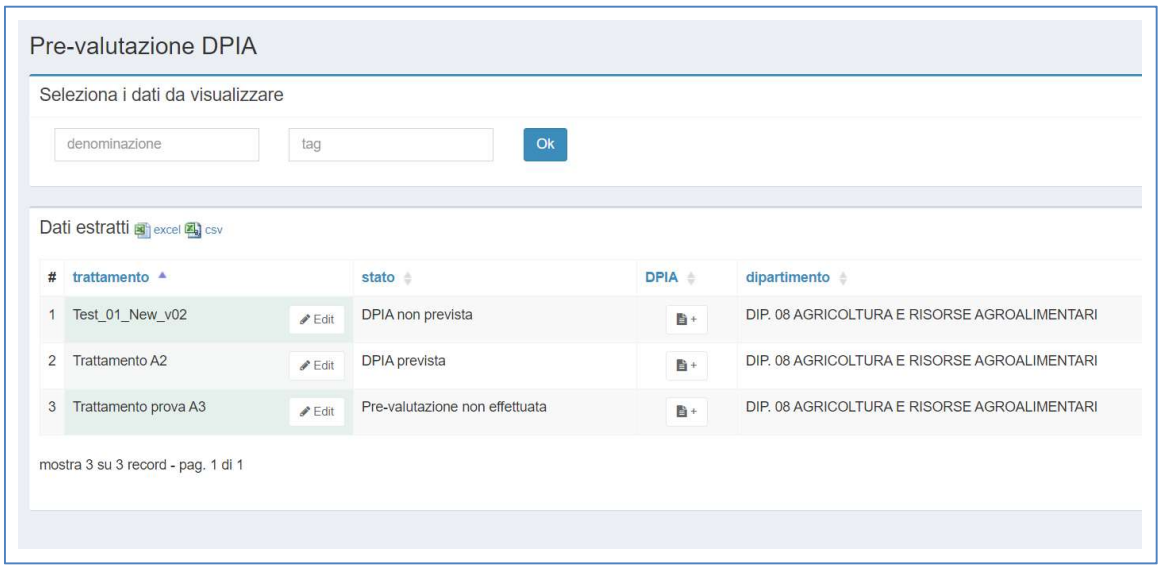


Figura 11 Tool Registri GDPR

Il Tool ARIEC è utilizzabile direttamente in locale eseguendo il file in formato MS Excel, introdotto come Allegato 2 del presente documento.

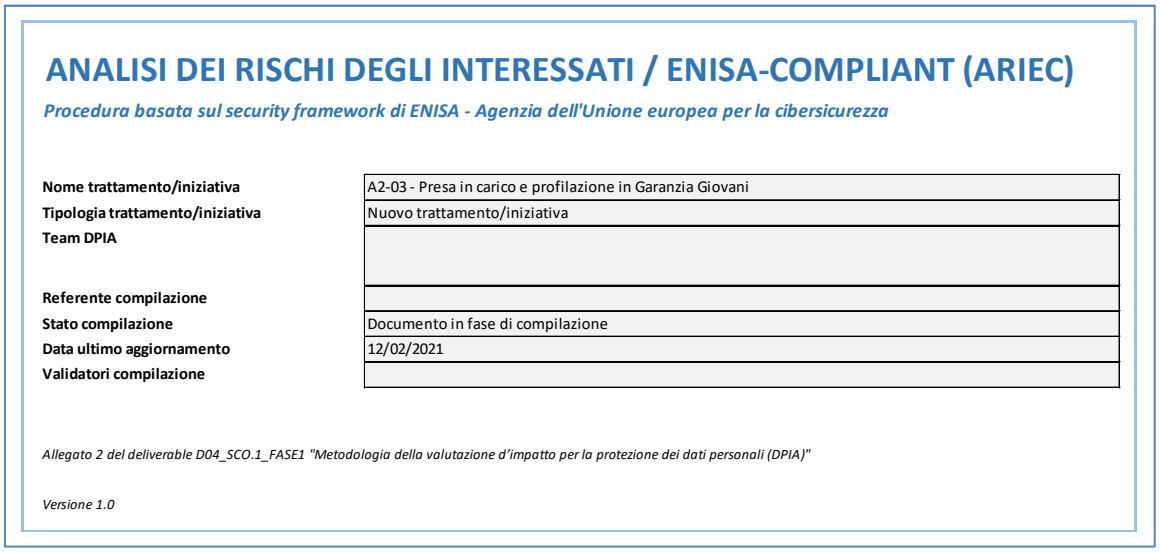


Figura 12 Tool ARIEC

7 ALLEGATO 1 - MISURE TECNICHE E ORGANIZZATIVE

Il presente lavoro è stato corredato di uno specifico documento a supporto dell'attività, descritta nella sezione 5.3.5, di selezione delle misure tecniche e organizzative da applicare al trattamento per mitigarne il rischio. Tale documento, dal titolo "MISURE TECNICHE E ORGANIZZATIVE", è riportato separatamente quale Allegato 1 del presente deliverable.

8 ALLEGATO 2 - TOOL ARIEC PER ANALISI DEI RISCHI

Il presente lavoro è stato corredato di uno specifico strumento a supporto della procedura, descritta nella sezione 5.3, di analisi dei rischi degli interessati. Tale strumento, basato su MS Excel e denominato "ANALISI DEI RISCHI DEGLI INTERESSATI / ENISA-COMPLIANT (TOOL ARIEC)", è riportato separatamente quale Allegato 2 del presente deliverable.

9 ALLEGATO 3 - MODELLO REPORT DPIA

Il presente lavoro è stato corredato di uno specifico modello per rappresentare efficacemente le risultanze dell'attività di DPIA. Tale documento, dal titolo "MODELLO REPORT DPIA", è riportato separatamente quale Allegato 3 del presente deliverable.