ANNA
LOBOSCO
19.11.2024
11:29:47
UTC

Michele
Emiliano
19.11.2024
16:46:08
GMT+02:00

R E G I O N E P U G L I A

Deliberazione della Giunta Regionale

N. 1528 del 18/11/2024 del Registro delle Deliberazioni

Codice CIFRA: AIG/DEL/2024/00004

OGGETTO: Definizione delle procedure interne di gestione delle attività di analisi dei rischi ex. artt. 24 e 32 GDPR e di valutazione di impatto (DPIA) ex art. 35 GDPR nell'ambito del trattamento di dati personali da parte delle Strutture Regionali.

L'anno 2024 addì 18 del mese di Novembre, si è tenuta la Giunta Regionale, previo regolare invito nelle persone dei Signori:

Sono presenti:		Nessuno assente.
Presidente	Michele Emiliano	
V.Presidente	Raffaele Piemontese	
Assessore	Fabiano Amati	
Assessore	Debora Ciliento	
Assessore	Alessandro Delli Noci	
Assessore	Sebastiano G. Leo	
Assessore	Gianfranco Lopane	
Assessore	Viviana Matrangola	
Assessore	Donato Pentassuglia	
Assessore	Giovanni F. Stea	
Assessore	Serena Triggiani	

Assiste alla seduta: la Segretaria Generale Dott.ssa Anna Lobosco

REGIONE PUGLIA

SEGRETERIA GENERALE DELLA PRESIDENZA

SEZIONE AFFARI ISTITUZIONALI E GIURIDICI

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA REGIONALE

Codice CIFRA: AIG/DEL/2024/00004

OGGETTO: Definizione delle procedure interne di gestione delle attività di analisi dei rischi *ex* artt. 24 e 32 GDPR e di valutazione di impatto (DPIA) *ex* art. 35 GDPR nell'ambito del trattamento di dati personali da parte delle Strutture Regionali.

Il Presidente della Giunta Regionale, sulla base dell'istruttoria espletata dalla E.Q. "Protezione dati personali nel Sistema Regione", confermata dal Dirigente della Sezione Affari istituzionali e giuridici anche in qualità di Responsabile Protezione Dati della Regione Puglia, e dal Segretario Generale della Presidenza della Giunta Regionale riferisce quanto segue:

Visti:

- La Deliberazione della Giunta Regionale 7 dicembre 2020, n. 1974, recante approvazione del nuovo Modello Organizzativo regionale "MAIA 2.0" e successive modifiche e integrazioni;
- Il Decreto del Presidente della Giunta Regionale 22 gennaio 2021, n. 22, recante adozione dell'Atto di alta organizzazione connesso al suddetto Modello organizzativo "MAIA 2.0" e successive modifiche e integrazioni;
- La Deliberazione della Giunta Regionale 15 settembre 2021, n. 1466, recante l'approvazione della Strategia regionale per la parità di genere, denominata "Agenda di Genere";
- La Deliberazione della Giunta Regionale 3 luglio 2023, n. 938, recante "D.G.R. n. 302/2022 "Valutazione di impatto di genere. Sistema di gestione e di monitoraggio". Revisione degli allegati".

Premesso che:

- Il Regolamento (UE) 2016/679 ("*General Data Protection Regulation*" - GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato essenzialmente sulla valutazione dei rischi inerenti i diritti e le libertà degli interessati, ha riformato il precedente impianto normativo nazionale in materia di protezione dei dati personali (D.Lgs. 196/2003, cd. "Codice Privacy"), inserendo come elemento cardine il principio di *"accountability"* ("responsabilizzazione") posto in capo al Titolare del trattamento, nonché ad eventuali Responsabili, i quali sono tenuti a garantire la conformità al GDPR di tutte le attività di trattamento dati e la tutela dei diritti dell'interessato attraverso l'adozione di misure tecniche ed organizzative adeguate ed efficaci, sottoposte a continuo aggiornamento;
- Il GDPR impone infatti ai Titolari di mettere in atto misure idonee a garantire ed attestare l'osservanza del citato Regolamento, tenendo conto, fra gli altri, dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (art. 24, par. 1);
- Ciascun trattamento di dati personali richiede obbligatoriamente una preliminare analisi dei rischi, come sancito dagli articoli 24, 25 e 32 del GDPR, il cui obiettivo è quello di valutare ogni possibile rischio connesso al trattamento, al fine di mettere in atto tutte le misure di sicurezza idonee a garantire il rispetto della vigente normativa;
- Dopo aver effettuato l'obbligatoria analisi dei rischi, per alcuni trattamenti di dati personali si renderà altresì necessaria la valutazione d'impatto (DPIA). L'esecuzione di tale valutazione d'impatto (cd. DPIA), da eseguire parimenti all'analisi dei rischi prima di procedere ad un trattamento, a differenza dell'analisi dei rischi non è sempre obbligatoria, ma deve essere effettuata nei casi espressamente previsti dalla normativa, ossia sostanzialmente quando il trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche. L'art. 35, par. 1 del GDPR prevede infatti che *"quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi"*; il medesimo art. 35, al successivo par. 3, dispone altresì che *"la valutazione d'impatto sulla protezione dei dati di cui al paragrafo, 1 è richiesta in particolare nei casi seguenti: a) 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; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

- Al fine di fornire indicazioni più concrete rispetto ai trattamenti che richiedono una DPIA a causa del rischio elevato rischio elevato per i diritti e le libertà delle persone fisiche, e tenendo conto degli elementi specifici contenuti nell'art. 35, par. 1 e 3, del GDPR innanzi citati, si richiamano i criteri dettati dal Comitato Europeo di Protezione dei Dati (*European Data Protection Board* – EDPB, già WP 29) nelle *"Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679"* adottate il 4 ottobre 2017, di seguito riportati :

"1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "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). A titolo esemplificativo si possono citare un istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio ovvero un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.

2. *Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura: trattamenti finalizzati ad assumere decisioni su interessati che producano "effetti giuridici sulla persona fisica" ovvero che "incidono in modo analogo significativamente su dette persone fisiche" (art. 35, paragrafo 3, lettera a)). Per esempio, il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio. Per maggiori dettagli sui concetti in gioco si rimanda alle Linee-guida in materia di profilazione che il Gruppo di lavoro si appresta a pubblicare.*
3. *Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico" (art. 35, paragrafo 3, lettera c)).14 Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità. Inoltre, è talora impossibile per gli interessati sottrarsi a questa tipologia di trattamenti in aree pubbliche (o pubblicamente accessibili).*
4. *Dati sensibili o dati di natura estremamente personale: si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10. A titolo di esempio, si può citare un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati. Al di là di queste disposizioni del regolamento, vi sono talune categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili (nell'accezione comune del termine), in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici dall'interessato ovvero da terzi. Il fatto che un certo dato personale sia disponibile pubblicamente può essere un elemento da prendere in esame*

nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi. Il criterio in oggetto può riferirsi anche a dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.

5. *Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala:*
   a) *numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;*
   b) *volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;*
   c) *durata, o persistenza, dell'attività di trattamento;*
   d) *ambito geografico dell'attività di trattamento.*
6. *Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.*
7. *Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, che. si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela(soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.*
8. *Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via. Il regolamento chiarisce (art. 35, paragrafo 1, e considerando 89 e 91) che l'utilizzo di una nuova tecnologia, definito "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare l'obbligo di condurre una DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia sono talora ignote. La DPIA aiuterà il titolare a comprendere e gestire tali rischi. Per esempio, alcune applicazioni legate all' "Internet delle cose" potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone, e, quindi, necessitano di una DPIA.*
9. *Tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto" (art. 22 e considerando 91). Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento".*

Sulla base delle richiamate Linee Guida EDPB/2017, ciascun Titolare *"può ritenere, nella maggioranza dei casi, che quando un trattamento soddisfa due dei criteri sopra indicati sia necessario condurre una DPIA. In linea di principio, il Gruppo di lavoro ritiene che quanto maggiore è il numero dei criteri soddisfatti da un determinato trattamento, tanto maggiore è la probabilità che esso presenti un rischio elevato per i diritti e le libertà degli interessati e, quindi, che si renda necessaria una DPIA indipendentemente dalle misure che il titolare prevede di adottare. Tuttavia, in taluni casi un titolare può ritenere che un trattamento che soddisfa solo uno dei criteri di cui sopra necessiti di una DPIA"*;

- Ad integrazione dei criteri per la redazione della DPIA definiti dalla Linee Guida EDPB innanzi citate, si richiama altresì l'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione

d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - contenuti nell'Allegato 1 del provvedimento dell'Autorità Garante Privacy (GPDP) n. 467 dell'11 ottobre 2018 [doc. Web n. 9058979], consultabile al seguente *link*: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9058979

- Il Titolare dovrà infine rivolgersi all'Autorità di controllo (Garante Privacy) per una consultazione preventiva, ai sensi dell'art. 36 del GDPR, qualora la valutazione di impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio medesimo.

Rilevato che:

- Con D.G.R. n. 145 del 30/1/2019 la Giunta Regionale della Puglia, in applicazione del disposto dell'art. 2-*quaterdecies* del D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679", ha delegato l'esercizio delle competenze del Titolare del trattamento in materia di protezione dei dati ai Dirigenti responsabili delle Strutture presso le quali si svolgono i singoli trattamenti, nominando questi ultimi "Designati del trattamento dei dati" e segnatamente definendone i relativi compiti;
- Sulla base delle previsioni della suddetta DGR n. 145/2019, i Dirigenti regionali – nella loro qualità di Designati al trattamento dei dati per le Strutture della Giunta regionale – sono tenuti, tra l'altro, ad *"adottare le misure tecniche ed organizzative per garantire la sicurezza dei dati. I dati personali, siano essi in formato digitale oppure su supporto cartaceo, devono essere custoditi con cura al fine di preservare le caratteristiche di disponibilità , autenticità, integrità e riservatezza. Il designato deve preoccuparsi, per quanto di competenza, dell'adozione delle misure di sicurezza adeguate e collaborare (…) nello svolgimento dell'analisi dei rischi, anche nei casi di cui all'art. 35 e 36 del Regolamento europeo relativi alla valutazione di impatto ed alla consultazione preventiva. Il Designato valuterà per la parte di propria competenza (…) le misure necessarie ai sensi dell'art. 32, tenendo conto della tipologia di dati e di operazioni nonché di quanto stabilito dall'art. 32".*

Considerato che:

- Il principio di "accountability" lascia al Titolare del trattamento non solo l'onere di determinare il rischio di impatto che il trattamento può avere sulla libertà e sui diritti degli interessati, ma anche di dimostrare che la valutazione di rischiosità e la conseguente scelta di misure tecnico/organizzative di sicurezza sia stata effettuata con metodologie chiare, efficaci e documentabili;
- Il GDPR non prevede, tuttavia, il *quomodo* in ordine alle modalità di attuazione del principio di *accountability*, lasciando libero il Titolare di definire le metodologie ritenute più opportune per l'analisi del rischio e per la valutazione d'impatto all'interno di ciascuna Amministrazione*;*

Ritenuto che:

- Si rende necessario disciplinare le procedure interne di gestione delle attività di Analisi dei Rischi *ex* artt. 24 e 32 GDPR e di Valutazione di impatto sulla protezione dei dati personali *ex* art. 35 GDPR, attraverso la validazione ed approvazione di modelli operativi che garantiscano l'applicazione di una metodologia oggettiva, chiara, efficace e documentabile, anche al fine di garantire modalità uniformi a livello regionale di effettuazione dell'Analisi dei Rischi e della Valutazione di Impatto.
- Tale regolamentazione si pone a supporto dei singoli dirigenti, Designati al trattamento ex DGR 145/2019, rendendo possibile una valutazione diretta ed immediata da parte di questi ultimi del livello di sicurezza e di conformità di ciascuno specifico trattamento alla vigente disciplina sulla protezione dei dati personali.

Si propone pertanto alla Giunta Regionale di adottare il "Modello di Analisi dei rischi nel trattamento dati personali (art. 24 e 32 GDPR)" ed il "Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR", elaborati con il supporto dell'Assistenza Tecnica Privacy regionale, rispettivamente Allegati A) e B) al presente schema di provvedimento per farne parte integrante e sostanziale.
Entrambi i modelli dovranno essere compilati direttamente a cura della Struttura regionale competente *ratione materiae*, con l'eventuale supporto dell'Assistenza Tecnica Privacy regionale, ed allegati all'interno del Registro Attività di Trattamento (RAT) in corrispondenza del trattamento di dati personali oggetto di analisi e valutazione.
Il "Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR", una volta compilato dalla Struttura regionale competente e prima dell'inserimento nel RAT, sarà trasmesso al DPO della Regione per il prescritto parere ai sensi dell'art. 35, par. 2 del GDPR regionale.
Le procedure interne e i correlati modelli adottati col presente schema di provvedimento saranno oggetto di apposita formazione rivolta a tutti i Dirigenti regionali, nella loro qualità di Designati al trattamento dei dati, ed ai Referenti privacy delle singole Strutture regionali, a cura del Responsabile Protezione Dati personali della Regione Puglia e con il supporto dell'Assistenza Tecnica Privacy regionale.

Garanzie di riservatezza

La pubblicazione sul BURP, nonché la pubblicazione all'Albo o sul sito istituzionale, salve le garanzie previste dalla Legge 241/1990 in tema di accesso ai documenti amministrativi, avviene nel rispetto della tutela della riservatezza dei cittadini secondo quanto disposto dal Regolamento UE n. 679/2016 in materia di protezione dei dati personali, nonché dal D.Lgs. 196/2003 ss.mm.ii., ed ai sensi del vigente Regolamento regionale 5/2006 per il trattamento dei dati sensibili e giudiziari, in quanto applicabile. Ai fini della pubblicità legale, il presente provvedimento è stato redatto in modo da evitare la diffusione di dati personali identificativi non necessari ovvero il riferimento alle particolari categorie di dati previste dagli articoli 9 e 10 del succitato Regolamento UE.

VALUTAZIONE DI IMPATTO DI GENERE

La presente deliberazione è stata sottoposta a Valutazione di impatto di genere ai sensi della DGR n. 398 del 03/07/2023.
L'impatto di genere stimato è:

- □ diretto
- □ indiretto
- ☒ neutro
- □ non rilevato

COPERTURA FINANZIARIA AI SENSI DEL D.LGS. 118/2011 s.m.i.

La presente deliberazione non comporta implicazioni, dirette e/o indirette, di natura economico-finanziaria e/o patrimoniale e dalla stessa non deriva alcun onere a carico del bilancio regionale.

Il Presidente, sulla base delle risultanze istruttorie come innanzi illustrate e motivate, ai sensi dell'art. 4, co. 4, lett. k) della L.R. n. 7/1997, propone alla Giunta Regionale:

- Di condividere quanto esposto in narrativa, che qui si intende integralmente riportato;
- Di disciplinare le procedure interne di gestione delle attività di Analisi dei Rischi *ex* artt. 24 e 32 GDPR e di Valutazione di impatto sulla protezione dei dati personali *ex* art. 35 GDPR, attraverso la validazione ed approvazione di modelli operativi che garantiscano l'applicazione di una metodologia oggettiva, chiara, efficace e documentabile, anche al fine di garantire modalità uniformi a livello regionale di effettuazione dell'Analisi dei Rischi e della Valutazione di Impatto.

- Di adottare, conseguentemente, il "*Modello di Analisi dei rischi nel trattamento dati personali (art. 24 e 32 GDPR)*" ed il "*Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR*", elaborati con il supporto dell'Assistenza Tecnica Privacy regionale, rispettivamente Allegati A) e B) al presente schema di provvedimento per farne parte integrante e sostanziale;
- Di disporre che i modelli adottati con il presente schema di provvedimento siano compilati direttamente a cura delle Strutture regionali competenti *ratione materiae*, con l'eventuale supporto dell'Assistenza Tecnica Privacy regionale, ed allegati all'interno del Registro Attività di Trattamento (RAT) in corrispondenza del trattamento di dati personali oggetto di analisi e valutazione. In particolare, il "Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR", una volta compilato dalla Struttura regionale competente e prima dell'inserimento nel RAT, dovrà essere trasmesso al DPO della Regione Puglia per il prescritto parere ai sensi dell'art. 35, par. 2 del GDPR regionale.
- Di dare atto che le procedure interne adottate col presente schema di provvedimento saranno fatte oggetto di apposita formazione rivolta a tutti i Dirigenti regionali, nella loro qualità di Designati al trattamento dei dati, ed ai Referenti privacy delle singole Strutture regionali, a cura del Responsabile Protezione Dati personali della Regione Puglia e con il supporto dell'Assistenza Tecnica Privacy regionale.
- Di trasmettere il presente schema di provvedimento ai Dirigenti della Regione Puglia nella loro qualità di Designati al trattamento ex DGR 145/2019;
- Di pubblicare il presente schema di provvedimento sul Bollettino Ufficiale della Regione Puglia ai sensi della L.R. n. 13/1994 s.m.i.;
- Di pubblicare il presente schema di provvedimento sul Portale web istituzionale regionale, all'interno della Sezione "Amministrazione Trasparente", Sottosezione "Disposizioni Generali/Atti generali/Atti amministrativi Generali".

I sottoscritti attestano che il procedimento istruttorio loro affidato è stato espletato nel rispetto della vigente normativa regionale, nazionale e comunitaria e che la seguente proposta di deliberazione, dagli stessi predisposto ai fini dell'adozione dell'atto finale da parte della Giunta regionale è conforme alle risultanze istruttorie.

Il Responsabile *ad interim* E.Q. "Protezione dati personali nel Sistema Regione"
Dott.ssa Maria Lucatorto

Maria Lucatorto
09.08.2024
13:23:58
GMT+02:00

Il Dirigente della Sezione Affari Istituzionali e Giuridici
Dott.ssa Rossella Caccavo

Rossella Caccavo
09.08.2024
13:06:58
GMT+02:00

Rossella Caccavo
13.11.2024
11:39:30
GMT+02:00

Il Segretario Generale della Presidenza
Dott. Roberto Venneri

Roberto Venneri
11.09.2024 16:08:19
GMT+02:00

Il Presidente della Giunta Regionale
Dott. Michele Emiliano

Michele Emiliano
11.11.2024
14:08:46
GMT+02:00

L A G I U N T A

- Udita la relazione e la conseguente proposta del Presidente;

- Viste le sottoscrizioni poste in calce alla proposta di deliberazione;

A voti unanimi espressi nei modi di legge

D E L I B E R A

- Di condividere quanto esposto in narrativa, che qui si intende integralmente riportato;
- Di disciplinare le procedure interne di gestione delle attività di Analisi dei Rischi *ex* artt. 24 e 32 GDPR e di Valutazione di impatto sulla protezione dei dati personali *ex* art. 35 GDPR, attraverso la validazione ed approvazione di modelli operativi che garantiscano l'applicazione di una metodologia oggettiva, chiara, efficace e documentabile, anche al fine di garantire modalità uniformi a livello regionale di effettuazione dell'Analisi dei Rischi e della Valutazione di Impatto.
- Di adottare, conseguentemente, il "*Modello di Analisi dei rischi nel trattamento dati personali (art. 24 e 32 GDPR)*" ed il "*Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR*", elaborati con il supporto dell'Assistenza Tecnica Privacy regionale, rispettivamente Allegati A) e B) al presente provvedimento per farne parte integrante e sostanziale;
- Di disporre che i modelli adottati con il presente provvedimento siano compilati direttamente a cura delle Strutture regionali competenti *ratione materiae*, con l'eventuale supporto dell'Assistenza Tecnica Privacy regionale, ed allegati all'interno del Registro Attività di Trattamento (RAT) in corrispondenza del trattamento di dati personali oggetto di analisi e valutazione. In particolare, il "Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR", una volta compilato dalla Struttura regionale competente e prima dell'inserimento nel RAT, dovrà essere trasmesso al DPO della Regione Puglia per il prescritto parere ai sensi dell'art. 35, par. 2 del GDPR regionale.
- Di dare atto che le procedure interne adottate col presente provvedimento saranno fatte oggetto di apposita formazione rivolta a tutti i Dirigenti regionali, nella loro qualità di Designati al trattamento dei dati, ed ai Referenti privacy delle singole Strutture regionali, a cura del Responsabile Protezione Dati personali della Regione Puglia e con il supporto dell'Assistenza Tecnica Privacy regionale.
- Di trasmettere il presente provvedimento ai Dirigenti della Regione Puglia nella loro qualità di Designati al trattamento ex DGR 145/2019;
- Di pubblicare il presente provvedimento sul Bollettino Ufficiale della Regione Puglia ai sensi della L.R. n. 13/1994 s.m.i.;
- Di pubblicare il presente provvedimento sul Portale web istituzionale regionale, all'interno della Sezione "Amministrazione Trasparente", Sottosezione "Disposizioni Generali/Atti generali/Atti amministrativi Generali".

Il Segretario Generale della Giunta	**Il Presidente della Giunta**

ALLEGATO A

REGIONE PUGLIA

Modello di Analisi dei rischi nel trattamento di dati personali (art. 24 e 32 GDPR)

REGIONE PUGLIA

TEAM DPO

Premessa

Il cosiddetto *risk-based thinking* è un approccio sistematico, strutturato e proattivo della gestione dei rischi, adottato da gran parte della recente normativa nazionale (vedi, ad es., il Testo Unico sulla Sicurezza (D.Lgs. 81/08) e comunitaria, a partire dal Reg. UE 679/2016 (GDPR), che disciplina il perimetro d'azione di riferimento con modalità basate sull'analisi dei rischi.

Il rischio, ovvero la verosimiglianza di accadimento di un evento avverso, incombe costantemente sui patrimoni informativi delle organizzazioni e, purtroppo, non è mai eliminabile del tutto; questo poiché sussiste sempre la possibilità di un incidente di sicurezza o, peggio, di un *data breach*, concretizzabile in qualunque momento del ciclo di vita delle informazioni. Per questo motivo è fondamentale, in ottica *privacy/security by design*, progettare le attività di trattamento in modo da ridurre la probabilità e gli eventuali impatti sulla vita, sulla dignità, sulle libertà e sulla riservatezza delle persone a cui i dati sono riferiti. Non esistono tuttavia in letteratura modelli standard di tipo oggettivo che possano guidare tale attività di analisi, né sono universalmente riconosciute specifiche procedure in grado di facilitare le operazioni preliminari di conformità alla disciplina sulla protezione dei dati personali.

Per questo motivo è stato redatto il presente modello di analisi del rischio, di tipo oggettivo, in modo che le Strutture regionali competenti *ratione materiae* – tenute a compilare il modello di analisi del rischio in questione – possano valutare immediatamente il livello di sicurezza e di conformità alla vigente disciplina sulla protezione dei dati personali di uno specifico trattamento, rendendo confrontabili i risultati nel tempo, anche in ottica di *accountability*.

Per l'utilizzo del presente modello di analisi non sono richieste particolari competenze tecniche o abilità, in quanto si tratta di una semplice lista di controllo alla quale associare alla colonna denominata "Misura tecnica organizzativa attiva" il valore "SI" nel caso la misura sia completamente attiva oppure il valore "NO" nel caso di assenza o attuazione parziale della medesima misura. Nel caso in cui la misura risulti invece non applicabile allo specifico contesto o al trattamento è possibile inserire il valore "N/A" (Non Applicabile).

In considerazione dei mutati scenari di rischio, delle tipologie e della numerosità di dati trattati, al fine di garantire un adeguato livello di sicurezza e conformità del trattamento, è auspicabile l'attivazione della maggior parte dei controlli previsti.

Il presente modello di analisi, sulla base dei principi-chiave posti a base di ciascuna misura (RISERVATEZZA/INTEGRITA'/DISPONIBILITA'/RESILIENZA/ACCOUNTABILITY) e del correlato impatto sull'attività amministrativa, nonché sulla base delle risposte fornite dall'operatore rispetto all'applicazione di ciascuna misura (SI/NO/NA), calcola automaticamente la probabilità ed il livello di rischio (*Risk rating* – BASSO/MEDIO/ALTO/ALTISSIMO) connessi. Alcune misure vanno considerate come irrinunciabili (riportate con il simbolo di spunta nella colonna "Misura obbligatoria") e l'eventuale parziale adozione/assenza della misura comporta un livello di rischio elevato e dunque non accettabile, indicato con la dicitura "NON ACCETTABILE" nella casella di intestazione del file denominata "LIVELLO DI RISCHIO COMPLESSIVO".

Considerato che l'attività di Analisi del rischio da effettuare con il presente modello risulta propedeutica alla redazione dell'eventuale Valutazione di impatto sulla protezione dei dati personali (DPIA) prevista all'art. 35 GDPR, si evidenzia che la condizione per poter procedere alla DPIA è che le risultanze dell'Analisi del rischio, punto di ingresso della valutazione di impatto, risultino comunque ad un livello ACCETTABILE.

Dunque, nel caso di livello NON ACCETTABILE del rischio complessivo, in ottica di *privacy by design*, non è possibile effettuare la DPIA, né tantomeno procedere con lo specifico trattamento dei dati personali. In tal caso, occorrerà intervenire preliminarmente sulle misure tecnico-organizzative attive, adottando le idonee misure non ancora attuate, al fine di ridurre il livello complessivo di rischio.

Modalità di compilazione

Il presente modello di analisi si avvale di uno strumento informatico in formato MS-Excel – riportato schematicamente in calce – che contiene una lista di misure di sicurezza tecniche ed organizzative, composta da n. 50 misure di sicurezza, di cui n. 25 di tipo organizzativo ed altrettante di tipo tecnico.

Nella compilazione del modello, è possibile selezionare una qualsiasi combinazione di misure attive, prestando particolare attenzione alle misure obbligatorie, contrassegnate dal pallino con la spunta ( ) nella colonna denominata "Misura obbligatoria": l'assenza o la parziale adozione di tali misure (indicata con "NO") comporta l'inaccettabilità del livello di rischio.

Il calcolo del livello di rischio complessivo è effettuato dinamicamente nell'ambito del modello, al mutare delle risposte fornite dal compilatore, rendendo subito evidenti le eventuali attività da porre in essere al fine di ridurre progressivamente i rischi connessi con i trattamenti e garantire al contempo gli adempimenti previsti. Nello specifico, il calcolo dei possibili impatti è calcolato per riga sulla bade degli elementi 'Riservatezza', 'Integrità', 'Disponibilità', 'Resilienza' e '*Accountability',* mentre la probabilità è calcolata per colonna, sempre in funzione della tipologia della singola misura di sicurezza. È quindi necessario completare l'inserimento delle informazioni relative a tutte le misure di sicurezza attive/adottate per ottenere un quadro di insieme coerente con gli obiettivi dell'analisi del rischio.

Le misure di sicurezza organizzative e tecniche sono identificate con una codifica (colonna "ID", con riportato "MO" per misura organizzativa e "MT" per misura tecnica) ed una descrizione. La colonna "Misura tecnica e organizzativa attiva" va compilata inserendo il valore "SI" nel caso di misura adottata e completamente attiva, oppure il valore "NO" nel caso di assenza o attuazione parziale della medesima misura. Nel caso in cui la misura risulti invece non applicabile allo specifico contesto o al trattamento è possibile inserire il valore "N/A" (Non Applicabile).

È possibile riportare, all'interno del modello, eventuali note volte ad esplicitare informazioni ritenute utili, come nell'esempio raffigurato in basso:

MO15	Applicazione della regola "prima trita, poi butta" per il personale autorizzato (nel caso di trattamenti in forma cartacea)	NO	in fase di attuazione
MO16	Applicazione della regola "non esporto dati dalla piattaforma applicativa" a meno di specifica autorizzazione, adottando particolari accortezze specie nel caso di dati particolari o elevata numerosità degli interessati o delle registrazioni	SI	

Nelle colonne successive alla colonna "Misura tecnica e organizzativa attiva", peraltro, sono presenti alcuni valori "di default" (raffigurati tramite pallini) connessi a ciascuna misura di sicurezza e non modificabili da parte del compilatore, necessari ai fini del calcolo.

Una volta completato l'inserimento delle informazioni richieste, il risultato dell'analisi è sintetizzato nella casella di intestazione del file denominata "LIVELLO DI RISCHIO COMPLESSIVO", come di seguito:

Nel caso di livello di rischio accettabile:

LIVELLO DI RISCHIO COMPLESSIVO:	ACCETTABILE

Nel caso di livello di rischio non accettabile:

LIVELLO DI RISCHIO COMPLESSIVO:	NON ACCETTABILE

In caso di non accettabilità del livello di rischio sarà necessario procedere con l'adozione delle misure di sicurezza tecniche o organizzative non ancora attuate, al fine di ridurre il livello complessivo di rischio, per poi procedere all'aggiornamento della compilazione del modello di analisi.

Richieste di supporto

Per eventuali chiarimenti o supporto operativo nella compilazione del presente modello di analisi del rischio è possibile contattare l'Assistenza Tecnica Privacy regionale al seguente indirizzo e-mail: assistenzatecnicaprivacy@regione.puglia.it .

Ai fini della più ampia diffusione dell'utilizzo consapevole del presente modello di analisi del rischio, sono previste delle sessioni formative dedicate rivolte a tutte le Strutture regionali, nell'ambito delle quali, accanto alla formazione teorica, saranno effettuate delle simulazioni operative di analisi del rischio.

LIVELLO DI RISCHIO COMPLESSIVO: ---

ID	Descrizione misura	Misura tecnica organizzativa attiva (Si/No)	Note	Riservatezza	Integrità	Disponibilità	Resilienza	Accountability	Prob. tot (1-5)	Impatto sulle attività amm. (1-5)	Misura obbligatoria	Rischio= f(Pt,I,Ril)	Risk rating (B/M/a/A)	Trattamento del rischio (Accettabile/ Da ridurre)
Misure di sicurezza organizzative														
MO01	Pubblicazione dell'informativa specifica nella sezione privacy del sito web istituzionale o nella piattaforma utilizzata per il trattamento							●		1	✓	-	---	
MO02	Pubblicazione informativa privacy "breve" nelle form on-line con rinvio alla informatica completa							●		1	✓	-	---	
MO03	Formalizzazione della nomina dei soggetti Autorizzati			●	●			●		3	✓	-	---	
MO04	Esecuzione della periodica verifica dell'ambito di autorizzazione degli utenti autorizzati			●	●			●		3	✓	-	---	
MO05	Formalizzazione della nomina dei Responsabili			●	●	●		●		4	✓	-	---	
MO06	Comunicazione al Titolare degli eventuali sub-Responsabili da parte del Responsabile			●				●		2		-	---	
MO07	Verifica periodica delle modalità di trattamento da parte dei Responsabili tramite attività di Audit di seconda parte			●	●	●	●	●		5		-	---	
MO08	Trattamento riportato nel RAT con almeno i seguenti "tab" compilati: Dati Generali, Responsabili Esterni, Persone Autorizzate, Categorie Dati Trattati e Base Giuridica, Categorie Trattamenti, Soggetti Interessati, Categorie Destinatari, Trasferimenti, Misure di Sicurezza, Asset, Archivi, Informativa							●		1	✓	-	---	
MO09	Formazione al personale autorizzato sui temi della protezione dei dati personali			●	●	●		●		4	✓	-	---	
MO10	Formazione al personale autorizzato verticalizzata sullo specifico trattamento			●	●	●		●		4		-	---	
MO11	Formalizzazione delle istruzioni sulle corrette modalità di trattamento al personale autorizzato			●	●	●		●		4	✓	-	---	
MO12	Attuazione della Regolamentazione generale sull'utilizzo dei sistemi e dispositivi informatici			●	●			●		3	✓	-	---	
MO13	Accesso alle aree di trattamento con supporti cartacei in modalità controllata, con porte e armadi chiusi a chiave			●	●			●		3		-	---	
MO14	Applicazione della regola "scrivania pulita" per il personale autorizzato (nel caso di trattamenti in forma cartacea)			●		●		●		3		-	---	
MO15	Applicazione della regola "prima trita, poi butta" per il personale autorizzato (nel caso di trattamenti in forma cartacea)			●				●		2		-	---	

MO16	Applicazione della regola “non esporto dati dalla piattaforma applicativa” a meno di specifica autorizzazione, adottando particolari accortezze specie nel caso di dati particolari o elevata numerosità degli interessati o delle registrazioni			●				●	2		-	---
MO17	Applicazione al personale autorizzato del divieto di riuso della carta già stampata			●				●	2		-	---
MO18	Definizione di una procedura alternativa di trattamento in caso di malfunzionamento della piattaforma informatica dedicata al trattamento specifico						●	●	2	✓	-	---
MO19	Implementazione del Piano di risposta agli incidenti di sicurezza e data breach						●	●	2	✓	-	---
MO20	Definizione dei tempi massimi di conservazione dei dati dello specifico trattamento (massimario di conservazione)			●				●	2	✓	-	---
MO21	Formalizzazione delle procedure di gestione (ad esempio, gestione account, backup e ripristino, manutenzioni e aggiornamenti, ecc.) da parte degli erogatori dei servizi informatici			●	●	●	●	●	5		-	---
MO22	Sensibilizzazione del personale ai temi della Sicurezza informatica			●	●	●		●	4	✓	-	---
MO23	Sensibilizzazione del personale al riconoscimento e segnalazione degli incidenti di sicurezza, violazione dei dati o Data Breach					●	●	●	3	✓	-	---
MO24	Formalizzazione della procedura di gestione della violazione dei dati o Data Breach					●	●	●	3	✓	-	---
MO25	Pubblicazione del modulo per l’esercizio dei diritti nella sezione privacy del sito web istituzionale							●	1	✓	-	---
Misure di sicurezza tecniche												
MT01	Implementazione della stratificazione delle autorizzazioni in piattaforma applicativa in funzione dei compiti assegnati			●	●			●	3		-	---
MT02	Implementazione di meccanismi di autenticazione forte a doppio fattore di autenticazione (SPID, CIE, EIDAS, TS), specie per i cittadini			●	●			●	3	✓	-	---
MT03	Implementazione di meccanismi di autenticazione forte a doppio fattore di autenticazione (token o app) per le connessioni VPN del personale o dei tecnici			●	●	●		●	4	✓	-	---
MT04	Adozione di credenziali dedicate con un elevato grado di complessità (password forti)			●	●	●		●	4		-	---
MT05	Adozione di politiche di modifica periodica ed obbligatoria delle credenziali			●				●	2		-	---
MT06	Disabilitazione automatica degli account inutilizzati da più di 3 mesi			●				●	2		-	---
MT07	Pubblicazione della piattaforma web dedicata al trattamento con protocollo sicuro “https”			●	●	●		●	4		-	---
MT08	Adozione e implementazione delle misure minime AgID (Circolare 2/2017)			●	●	●	●	●	5	✓	-	---
MT09	Piattaforma software SaaS qualificata secondo le prescrizione dell’Agenzia per la cybersicurezza nazionale				●	●	●	●	4		-	---

MT10	Fornitori dei servizi certificati ISO/IEC 27001			●	●	●	●	●	5		-	---
MT11	Esecuzione delle copie di sicurezza e di una “copia sterile” (off-line) almeno giornalmente					●	●	●	3	✓	-	---
MT12	Esecuzione dei test periodici di ripristino delle copie di sicurezza					●	●	●	3	✓	-	---
MT13	Implementazione degli Audit log (verifica automatica di eventuali comportamenti anomali degli utenti autorizzati) e attivazione di allarmi nel caso di attacchi o attività insolite			●			●	●	3		-	---
MT14	Aggiornamento periodico della piattaforma applicativa dedicata					●	●	●	3	✓	-	---
MT15	Aggiornamento periodico del sistema operativo e dei componenti dei sistemi server utilizzati					●	●	●	3	✓	-	---
MT16	Geo-limitazione della visibilità in rete della piattaforma applicativa alla sola Regione Puglia o Italia (piattaforma non raggiungibile da altri paesi UE o extra UE)			●	●			●	3		-	---
MT17	Limitazione oraria (festivi esclusi) della visibilità in rete della piattaforma applicativa			●	●			●	3		-	---
MT18	Attivazione di allarmi nel caso di attacchi o attività insolite						●	●	2	✓	-	---
MT19	Attivazione di un sistema di monitoraggio della funzionalità base (risposta a chiamata) e delle performance					●	●	●	3		-	---
MT20	Registrazione delle attività degli utenti a livello di piattaforma			●				●	2	✓	-	---
MT21	Valutazione periodica delle eventuali vulnerabilità della piattaforma applicativa e della sottostante catena tecnologica				●	●		●	3	✓	-	---
MT22	Separazione degli ambienti di test e produzione (non sono caricati dati reali negli ambienti di test)			●				●	2		-	---
MT23	Attivazione di sistemi antivirus / anti-malware sui sistemi client e server				●	●		●	3	✓	-	---
MT24	Training periodico del Piano di risposta agli incidenti e data breach						●	●	2		-	---
MT25	Training periodico del Piano di continuità operativa						●	●	2		-	---

ALLEGATO B

REGIONE PUGLIA

Modello per la redazione della Valutazione di impatto (DPIA) ex art. 35 GDPR nel trattamento di dati personali

Redazione Valutazione di impatto (DPIA) - Informazioni necessarie

Al fine di poter effettuare correttamente la Valutazione di impatto (DPIA) relativa ad uno specifico trattamento, come previsto dall'attuale disciplina sulla protezione dei dati personali (art. 35 GDPR), è necessario fornire le informazioni e la documentazione di seguito riportate.

***NOTA**: I campi contrassegnati con l'asterisco (*) sono obbligatori; l'assenza di uno o più elementi obbligatori potrebbe comportare l'impossibilità di procedere alla gestione della richiesta.*

In caso di dubbi ovvero di necessità di supporto alla compilazione è possibile contattare direttamente l'Assistenza tecnica del DPO regionale (e-mail assistenzatecnicaprivacy@regione.puglia.it) che fornirà tutte le delucidazioni necessarie.

Soggetti di riferimento del trattamento (*processo/progetto/intervento/azione*):

Ruolo *	**Nominativo** *	**E-mail** *	**Tel.** *(diretto/mobile)* *
Designato * ***(dirigente competente per materia)***			
Referenti * ***(soggetti interni alla Struttura regionale competente per materia, ad es., funzionario, RUP, ecc., incaricato del procedimento/ trattamento dei dati personali)***			

Definizione del trattamento	
Denominazione Trattamento Dati Personali *	*Riportare la denominazione del trattamento (campo Trattamento Dati Personali) così come inserita nell'applicativo software "Registro delle attività di trattamento dei dati" di cui alla DGR 2159/2021 – RAT (https://gdpr.regione.puglia.it).* ***[Nota**: Si suggerisce di effettuare un "copia e incolla" del testo dal RAT, al fine di permettere l'identità terminologica propedeutica alla corretta identificazione del trattamento].*
Descrizione del trattamento *	*Riportare una breve descrizione del trattamento, con indicazione del flusso delle informazioni, delle eventuali interconnessioni con altri titolari o della delega ai Responsabili delle attività di trattamento.*
Normativa e disposizioni di riferimento *	*Leggi e Regolamenti regionali, nazionali e comunitari, Atti amministrativi, Direttive, Circolari (tali norme e disposizioni devono essere espressamente richiamate, ed eventualmente allegate alla valutazione: **in caso contrario non si potrà procedere alla redazione della DPIA**).*

Motivo di redazione della DPIA	
Motivo di redazione della DPIA *	*Specificare le motivazioni di redazione della DPIA:* La DPIA risulta **obbligatoria** nel caso di risposta affermativa ad **almeno 2 dei seguenti quesiti**, mentre risulta facoltativa nel caso di risposta affermativa ad almeno 1 dei seguenti quesiti (Provvedimento WP-29 n. 248 del 4 ottobre 2017): ☐ I dati personali trattati servono a fare valutazioni o ad assegnare punteggi ? ☐ I dati personali trattati servono a prendere decisioni automatiche ?

Motivo di redazione della DPIA	
	☐ I dati personali trattati servono per il monitoraggio sistematico dell'interessato ? ☐ Si trattano dati personali sensibili o dati aventi carattere altamente personale (dati riguardanti la salute, l'orientamento sessuale, le opinioni religiose, politiche o sindacali, le condanne penali o i reati, ecc.) ? ☐ Si trattano dati personali su larga scala, dal punto di vista sia del numero dei soggetti interessati al trattamento che del volume dei dati trattati ? ☐ I dati personali trattati sono frutto di combinazioni di più fonti (ad es. dati derivanti da due o più operazioni di trattamento e/o da titolari del trattamento diversi? ☐ I dati personali trattati riguardano soggetti vulnerabili ? ☐ I dati personali sono trattati per mezzo di nuove tecnologie evolute e/o nuove soluzioni organizzative ? ☐ Il trattamento dei dati personali può impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto ? *Ai fini di una valutazione approfondita in ordine alla necessità di redazione della DPIA, si richiamano altresì i criteri contenuti nell'Allegato 1 al provvedimento dell'Autorità Garante Privacy (GPDP) n. 467 dell'11 ottobre 2018 [doc. Web n. 9058979], di seguito riportati*: 1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti 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". 2. Trattamenti automatizzati finalizzati 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). 3. Trattamenti che prevedono 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 il trattamento 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. 4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, 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). 5. Trattamenti effettuati 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 WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8). 6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo). 7. Trattamenti effettuati 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*) ogniqualvolta ricorra

Motivo di redazione della DPIA	
	anche almeno un altro dei criteri individuati nel WP 248, rev. 01 . 8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche. 9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*). 10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR interconnessi con altri dati personali raccolti per finalità diverse. 11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento. 12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Requisiti minimi *		
Informativa privacy * *(artt. 12, 13, 14)*	*Fornire **in allegato** l'informativa verticalizzata sul trattamento oggetto di DPIA, completa e/o in formato breve (ad esempio, riportata nella modulistica o pubblicata in piattaforma online).*	*Modalità di ostensione prevista*: ☐ sito web istituzionale/tematico; ☐ piattaforma online dedicata al trattamento; ☐ disponibilità/consegna diretta al singolo interessato; ☐ altro: _____.
Nomina soggetti autorizzati *	*Tutti i soggetti deputati al trattamento devono essere specificatamente autorizzati.*	*Modalità di autorizzazione*: ☐ nomina singolo soggetto autorizzato; ☐ nomina funzionale per appartenenza alla struttura regionale/UO competente.
Soggetti coinvolti nel trattamento dei dati personali *	Titolare:	Regione Puglia
	Contitolare (eventuale):	
	Designati:	Dirigente Struttura _____.
	Responsabili:	☐ InnovaPuglia S.p.A. ☐ ☐
	Sub-Responsabili del trattamento (specificare):	
Nomina Responsabili *	*I soggetti giuridici che effettuano attività per conto del Titolare del trattamento (fornitori, gestori di servizi, ecc.) devono essere nominati con accordo ai sensi dell'art. 28 GDPR rispetto allo specifico trattamento; tali soggetti, cui devono essere fornite idonee istruzioni relative alle modalità di svolgimento del trattamento, hanno l'obbligo di adottare le misure di sicurezza tecniche e organizzative necessarie rispetto alla tipologia di dati trattati e ai rischi incombenti, unitamente all'obbligo legale di riservatezza del personale impiegato nel trattamento medesimo.*	*Modalità di nomina*: ☐ Contestualmente alla firma del contratto/ convenzione/protocollo d'intesa; ☐ Non sono delegate a soggetti terzi attività di trattamento di dati personali; ☐ Altro (specificare): _____.
Analisi del rischio *	*L'analisi del rischio deve essere effettuata in via propedeutica rispetto alla DPIA – attraverso il "**Modello di Analisi dei Rischi" allegato** (All. A) – ed il relativo*	Risultato dell'Analisi del rischio: ☐ **ACCETTABILE**

Requisiti minimi *		
	*esito in termini di "LIVELLO DI RISCHIO COMPLESSIVO" deve essere "**ACCETTABILE**".* *Nel caso in cui il livello di rischio complessivo risulti **NON ACCETTABILE**, si dovrà procedere – preliminarmente all'effettuazione della DPIA – con l'adozione di ogni ulteriore misura tecnica e organizzativa prevista dal modello che consenta di arrivare all'accettabilità del rischio [livello di rischio "ACCETTABILE"].* ***La suddetta analisi del rischio va obbligatoriamente allegata alla DPIA**.*	

Elementi necessari per la valutazione dei rischi * (*indicare almeno una delle tre tipologie contemplate*)		
Piattaforme informatiche utilizzate nel trattamento	*Riportare gli indirizzi web (URL) delle piattaforme informatiche utilizzate, sia regionali che esterne (ad es., https://<xyz>.regione.puglia.it).*	
Asset utilizzati	*Indicare gli altri applicativi software utilizzati (ad esempio, software installati localmente o condivisioni di rete, file hosting, ecc.).*	
	Indicare i sistemi o dispositivi hardware utilizzati (portatili, tablet, smartphone, IoT, ecc.).	
Supporti cartacei	*Indicare le modalità di trattamento su supporto cartaceo eventualmente effettuate, inclusa la conservazione.*	

Di seguito gli elementi da selezionare o riportare al fine di permettere la corretta redazione della DPIA, verificando sempre l'allineamento con quanto riportato nel RAT per il trattamento in questione:

Valutazione di impatto (DPIA) - Informazioni generali			
Tipologia di operazioni effettuate sui dati personali: *	☐ raccolta	☐ registrazione	☐ organizzazione
	☐ conservazione	☐ adattamento	☐ modifica
	☐ consultazione	☐ comunicazione	☐ trasmissione
	☐ messa a disposizione	☐ raffronto	☐ interconnessione
	☐ cancellazione	☐ distruzione	
Dati personali trattati *	*Indicare le macrocategorie di dati personali trattati:*	☒ Dati comuni (*nominativo, indirizzo, e-mail, telefono, , ecc.*); ☐ Dati particolari [*art. 9 GDPR*] ☐ Origine razziale o etnica; ☐ Opinioni politiche; ☐ Convinzioni religiose o filosofiche; ☐ Appartenenza sindacale;	

		☐ Dati genetici; ☐ Dati biometrici; ☐ Dati relativi alla salute; ☐ Dati relativi alla vita sessuale; ☐ Dati relativi all'orientamento sessuale. ☐ Dati soggetti a maggiore tutela dell'anonimato (*relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all'uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari*) ["Linee guida in materia di dossier sanitario" - Allegato A alla deliberazione del Garante Privacy del 4 giugno 2015; art. 6, D.M. Ministro della Salute del 7.9.2023 - "Fascicolo Sanitario Elettronico 2.0"]; ☐ Dati giudiziari [*art. 10 GDPR*].
	Esplicitare la tipologia/ambito di riferimento dei dati personali trattati:	☐ Famiglia o situazioni personali; ☐ Lavoro (*occupazione attuale e precedente, curriculum, ecc.*); ☐ Istruzione e cultura (*diploma, laurea, attestati, ecc.*); ☐ Documento di riconoscimento; ☐ Documenti reddituali (*dichiarazione dei redditi, buste paga, ecc.*); ☐ Dati patrimoniali reddituali finanziari e assicurativi; ☐ Residenza e recapiti (*indirizzo, mail, telefono, coordinate bancarie, ecc.*); ☐ Altro: _____
Natura del trattamento	*Indicare eventuali caratteristiche intrinseche del trattamento che possano rappresentare un rischio rilevante per gli interessati [EDPB Guidelines 2019-04 Data protection by design and by default, v. 2.0]:*	☐ Processo decisionale automatizzato; ☐ Rapporti di forza asimmetrici; ☐ Imprevedibilità del trattamento; ☐ Difficoltà per l'interessato di esercitare i propri diritti; ☐ Altro: _____
Ambito di applicazione	*Indicare la dimensione (potenziale) del trattamento:*	☐ 1 – 1.000 interessati ☐ 1.000 – 10.000 interessati ☐ 10.000 – 100.000 interessati ☐ Oltre 100.000 interessati ☐ Non definito/definibile
Materia	*Indicare la materia relativa al trattamento dei dati personali:*	☐ Agricoltura, sviluppo rurale e ambientale ☐ Ambiente, paesaggio e qualità urbana ☐ Bilancio, affari generali ed infrastrutture ☐ Mobilità ☐ Personale e organizzazione ☐ Politiche del lavoro, istruzione e formazione ☐ Promozione della salute e del benessere animale ☐ Sviluppo economico ☐ Turismo, economia della cultura e valorizzazione del territorio ☐ Protezione civile e gestione delle emergenze ☐ Welfare ☐ Gestione e controllo dei fondi europei ☐ Avvocatura regionale ☐ Politiche internazionali ☐ Appalti e contratti ☐ Comunicazione istituzionale

		☐ Attività del Gabinetto del Presidente e della Segreteria Generale della Presidenza ☐ Attività della Giunta Regionale ☐ Altro _____
Valutazione delle misure atte a garantire necessità e proporzionalità del trattamento *[art. 35, paragrafo 7, lettera b) GDPR]*		
Finalità *	*Descrivere le finalità del trattamento:*	
Condizioni di liceità del trattamento *	*Indicare la base giuridica ai sensi dell'art. 6 GDPR relativamente ai dati personali comuni :* *[**in grassetto** la base giuridica tipica delle Pubbliche Amministrazioni]*	☐ consenso dell'interessato [*art. 6, par. 1, lett. a) GDPR*] (*da considerarsi del tutto residuale nell'ambito PA).* ☐ esecuzione di un contratto o di misure precontrattuali [art. *6, par. 1, lett. b) GDPR*]; ☐ **obbligo legale [*art. 6, par. 1, lett. c) GDPR*]**; ☐ salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica [*art. 6, par. 1, lett. d) GDPR*]; ☐ **compito di interesse pubblico o connesso all'esercizio di pubblici poteri [*art. 6, par. 1, lett. e) GDPR*]**; ☐ perseguimento del legittimo interesse del titolare del trattamento o di terzi [*art. 6, par. 1, lett. f) GDPR*] (esempio, videosorveglianza);
	Indicare la base giuridica ai sensi dell'art. 9 GDPR relativamente alle particolari categorie di dati personali (ex dati sensibili), ove trattati: *[**in grassetto** la base giuridica tipica delle Pubbliche Amministrazioni]*	☐ consenso dell'interessato [*art. 9, par. 2, lett. a) GDPR*] (*da considerarsi del tutto residuale nell'ambito PA*); ☐ trattamento necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale [*art. 9, par. 2, lett. b) GDPR*]; ☐ trattamento necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica [*art. 9, par. 2, lett. c) GDPR*]; ☐ trattamento riguardante dati personali resi manifestamente pubblici dall'interessato [*art. 9, par. 2, lett. e) GDPR*]; ☐ trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria [*art. 9, par. 2, lett. f) GDPR*]; ☐ **trattamento necessario per motivi di interesse pubblico rilevante [*art. 9, par. 2, lett. g) GDPR*];** ☐ trattamento necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali [*art. 9, par. 2, lett. h) GDPR*]; ☐ **trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici [*art. 9, par. 2, lett. i) GDPR*]; ☐ trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici [*art. 9, par. 2, lett. j) GDPR*].
	Indicare la base giuridica ai sensi dell'art. 2-sexies D.lgs. 196/03 relativamente ai dati di natura particolare (sensibili), ove trattati, in	☐ accesso a documenti amministrativi e accesso civico [*art. 2-sexies lett. a) D.lgs. 196/03*]; ☐ tenuta di registri pubblici relativi a beni immobili o mobili civico [*art. 2-sexies lett. c) D.lgs. 196/03*];

	caso di trattamenti effettuati per motivi di interesse pubblico rilevante :	☐ cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato [*art. 2-sexies lett. e) D.lgs. 196/03*]; ☐ elettorato attivo e passivo ed esercizio di altri diritti politici, documentazione delle attività istituzionali di organi pubblici, redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari [*art. 2-sexies lett. f) D.lgs. 196/03*]; ☐ esercizio del mandato degli organi rappresentativi, cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche [*art. 2-sexies lett. g) D.lgs. 196/03*]; ☐ svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo [*art. 2-sexies lett. h) D.lgs. 196/03*]; ☐ attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale [*art. 2-sexies lett. i) D.lgs. 196/03*]; ☐ attività di controllo e ispettive [*art. 2-sexies lett. l) D.lgs. 196/03*]; ☐ concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni [*art. 2-sexies lett. m) D.lgs. 196/03*]; ☐ conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali[*art. 2-sexies lett. n) D.lgs. 196/03*]; ☐ rapporti tra i soggetti pubblici e gli enti del terzo settore [*art. 2-sexies lett. o) D.lgs. 196/03*]; ☐ attività sanzionatorie e di tutela in sede amministrativa o giudiziaria [*art. 2-sexies lett. q) D.lgs. 196/03*]; ☐ rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose [*art. 2-sexies lett. r) D.lgs. 196/03*]; ☐ attività socioassistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci [*art. 2-sexies lett. s) D.lgs. 196/03*]; ☐ programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale [*art. 2-sexies lett. v) D.lgs. 196/03*]; ☐ tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili [*art. 2-sexies lett. aa) D.lgs. 196/03*]; ☐ istruzione e formazione in ambito scolastico, professionale, superiore o universitario [*art. 2-sexies lett. bb) D.lgs. 196/03*];

		☐ trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan) [*art. 2-sexies lett. cc) D.lgs. 196/03*]; ☐ Instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva [*art. 2-sexies lett. dd) D.lgs. 196/03*].
Condizioni di liceità del trattamento dei dati giudiziari	*Indicare la base giuridica ai sensi degli artt. 5 e 7 D.lgs. 51/2018 relativamente ai dati di natura giudiziaria di cui all'art. 10 GDPR, ove trattati, in caso di trattamenti effettuati per:*	☐ prevenzione, indagine, accertamento e perseguimento di reati; ☐ esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.
	Indicare la base giuridica ai sensi dell'art. 2-octies D.lgs. 196/03 relativamente ai dati di natura giudiziaria, ove trattati, in caso di trattamenti effettuati per:	☐ Adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del GDPR [*art. 2-octies lett. a) D.lgs. 196/03*]; ☐ Adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali [*art. 2-octies lett. b) D.lgs. 196/03*]; ☐ Verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti [*art. 2-octies lett. c) D.lgs. 196/03*]; ☐ Accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia [*art. 2-octies lett. d) D.lgs. 196/03*]; ☐ Accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria [*art. 2-octies lett. e) D.lgs. 196/03*]; ☐ Esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia [*art. 2-octies lett. f) D.lgs. 196/03*]; ☐ Esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza [*art. 2-octies lett. g) D.lgs. 196/03*]; ☐ Adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di

		altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto [*art. 2-octies lett. h) D.lgs. 196/03*]; ☐ Accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti [*art. 2-octies lett. i) D.lgs. 196/03*]; ☐ Attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese ai sensi dell'articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27 [*art. 2-octies lett. l) D.lgs. 196/03*]; ☐ Adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo[*art. 2-octies lett. m) D.lgs. 196/03*].
Adeguatezza, pertinenza e non eccedenza (*art. 5, par. 1, lettera c) GDPR*)	*Indicare le misure poste in essere al fine di garantire adeguatezza (efficacia della protezione dei dati):*	☐ sistema di gestione della sicurezza delle informazioni; ☐ analisi del rischio effettuata; ☐ applicati principi di *security/privacy by design;* ☐ verifiche periodiche sui sistemi/piattaforme (VA/PT); ☐ controllo degli accessi (*need to know, need to do*); ☐ limitazione dell'accesso (degli operatori e rispetto ai contenuti); ☐ segregazione dell'accesso; ☐ trasferimenti protetti e sicuri; ☐ conservazione sicura; ☐ pseudonimizzazione; ☐ backup e repliche; ☐ registrazione continua degli eventi e delle azioni (log); ☐ piano di disaster recovery/continuità operativa; ☐ procedura di data breach e risposta agli incidenti.
	Indicare le misure poste in essere al fine di garantire la pertinenza (correttezza della base giuridica):	☐ effettuata e mantenuta aggiornata la mappatura dei trattamenti; ☐ applicata la corretta base giuridica, validata con il DPO; ☐ base giuridica differenziata per ciascuna attività di trattamento; ☐ trattamento necessario e non soggetto a condizioni; ☐ piena autonomia dell'interessato nel controllo dei propri dati personali; ☐ base giuridica predeterminata prima dell'inizio del trattamento; ☐ cessazione del trattamento nel caso di base giuridica non più valida; ☐ adeguamento del trattamento rispetto alla eventuale modifica della base giuridica.
	Indicare le misure poste in essere al fine di garantire la non eccedenza (principio di necessità), anche in logica di privacy by design:	☐ i dati trattati, le funzioni e i profili di autorizzazione sono predeterminati prima dell'inizio del trattamento; ☐ i dati trattati sono stati minimizzati e validati come nucleo minimo; ☐ sono effettuate verifiche periodiche in relazione ai dati trattati, alle funzioni e ai profili di autorizzazione.
Esattezza e aggiornamento dei dati	*Indicare eventuali misure poste in essere al fine di garantire esattezza e*	☐ fonti dei dati personali affidabili (per dati acquisiti non direttamente dall'interessato); ☐ correttezza dei dati personali verificata periodicamente;

(art. 5, par. 1, lettera d) GDPR)	*aggiornamento dei dati.*	☐ cancellazione/rettifica tempestiva dei dati su richiesta dell'interessato secondo procedura; ☐ effetto della propagazione di errori ridotto grazie ai controlli; ☐ aggiornamento dei dati da parte dell'interessato secondo prevista procedura; ☐ in fase di acquisizione sono previste soltanto scelte concise e predeterminate anziché campi a testo libero.
Periodo di conservazione dei dati personali * *[NOTA - Occorre compilare obbligatoriamente la prima riga (tempi di conservazione), oppure in alternativa, solo in caso di tempi non definiti, la seconda riga (criteri di determinazione dei tempi)].*	*Indicare le tempistiche previste di conservazione dei dati personali:*	Numero anni: _____. *Fonte:* ☐ fonte normativa o amministrativa; ☐ manuale di conservazione documentale regionale; ☐ altro:_____.
	Criteri per determinare il periodo di conservazione, nel caso in cui il numero di anni non sia determinabile con esattezza:	☐ cancellazione automatica alla conclusione del trattamento; ☐ legato a specifiche necessità e finalità: _____; ☐ altro: _____.
Valutazione delle misure atte a garantire i diritti degli interessati		
Esercizio dei diritti	*Indicare le previste modalità di esercizio dei diritti:*	☐ procedura di accesso (art. 15); ☐ procedura di rettifica (art. 16); ☐ procedura di obbligo di notifica (art. 19); ☐ procedura di limitazione e opposizione trattamento (art. 18, 19 e 21).
Garanzie riguardanti l'eventuale trasferimento dei dati personali in Paesi terzi * *(Capo V GDPR)*	*Indicare se sono effettuati trasferimento dei dati personali in Paesi esteri e quali misure sono poste in essere a garanzia dei diritti degli interessati.*	☐ Sono previsti trasferimenti di dati personali fuori dalla UE. *In caso di trasferimenti extra UE, sono previste le seguenti misura di conformità al trasferimento extra UE:* ☐ decisioni di adeguatezza [*art. 45 GDPR*]; ☐ strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici [*art. 46, par. 2, lett. a GDPR*]; ☐ norme vincolanti d'impresa [*art. 46, par. 2, lett. b*]; ☐ clausole tipo [*art. 46, par. 2, lett. c e lett. d*]; ☐ codici di condotta [*art. 46, par. 2, lett. e*]; ☐ meccanismi di certificazione [*art. 46, par. 2, lett. f*]; ☐ consenso degli interessati (*da considerarsi del tutto residuale nell'ambito PA).* *Previa autorizzazione del Garante:* ☐ clausole contrattuali *ad hoc* [*art. 46, par. 3, lett. a*]; ☐ accordi amministrativi tra autorità o organismi pubblici [*art. 46, par. 3, lett. b].*
Consultazione preventiva * *(art. 36 GDPR)*	*Riportare se è stata effettuata, anche precedentemente, una consultazione preventiva presso l'Autorità Garante.*	☐ Effettuata consultazione preventiva presso l'Autorità Garante; ☐ non effettuata consultazione preventiva presso l'Autorità Garante.

Altre informazioni utili alla valutazione	
Opinioni degli interessati o dei loro rappresentanti eventualmente raccolte *(art. 35, par. 9)*	☐ Non si è ritenuto necessario richiedere parere agli interessati, pur restando fermo l'ascolto di ogni istanza da parte dei loro rappresentanti. ☐ Il parere degli interessati è il seguente:
Note	

Parere DPO *[spazio riservato al DPO]*	
Parere del DPO	☐ **PARERE FAVOREVOLE** ☐ **FAVOREVOLE CONDIZIONATO A**: _____ ☐ **PARERE NEGATIVO**
Motivazioni del parere	

Rossella Caccavo
09.08.2024
13:06:57
GMT+02:00