ALLEGATO QQ ([1])

DATA PROTECION IMPACT ASSESSMENT (DPIA) POLICY

[1] Allegato aggiunto dall'articolo 12, comma 1, del r.r. 4 aprile 2025, n. 8, pubblicato sul BUR Lazio 8 aprile 2025, n. 28.

Sommario

1. PREMESSA

Il Regolamento (UE) 679/2016 (di seguito "RGPD") ha introdotto nuove regole in tema di protezione dei dati personali che prevedono, tra l'altro, la necessità che il Titolare del trattamento sin dal momento di determinare i mezzi del trattamento e per tutta la durata dello stesso, metta in atto misure tecniche e organizzative finalizzate ad attuare in modo efficace i principi di protezione dei dati e adotti garanzie adeguate a soddisfare i principi del RGPD e a tutelare i diritti degli interessati.

Lo scopo principale della presente *policy*, in ossequio al principio di *Privacy by design e by default,* (di seguito "PBDD") stabilito dall'articolo 25 del RGPD, è quello di descrivere le modalità di esecuzione della valutazione d'impatto sulla protezione dei dati (c.d. *Data protection Impact Assessment* di seguito "DPIA") ai sensi dell'art. 35 RGPD.

2. AMBITO DI APPLICAZIONE

La presente *policy* si applica alla Giunta regionale del Lazio (di seguito "Giunta" o "Titolare") in qualità di Titolare del trattamento secondo le responsabilità e i ruoli definiti nel modello organizzativo regionale in materia di protezione dei dati personali di cui al Titolo IX, Capo V del Regolamento Regionale n.1/2002 e successive modifiche e integrazioni.

Il Titolare, in conformità al principio di responsabilizzazione di cui all'art. 5, par. 2, RGPD ("*Accountability*") e al principio di Privacy *by design e by default* di cui all'art. 25 RGPD, in presenza di un rischio elevato per gli interessati e in tutti gli altri casi previsti dall'art. 35 del RGPD, è tenuta, prima dell'inizio delle attività del trattamento, ad eseguire una DPIA.

3. ABBREVIAZIONI E ACRONIMI

- **RGPD*:*** *Reg. UE 2016/679 "Regolamento generale sulla protezione dei dati" (anche GDPR "General Data Protection Regulation");*
- **WP29*:*** *Working Party Article 29 (Gruppo Articolo 29).*

4. DEFINIZIONI

Di seguito si riportano le definizioni dei principali termini utilizzati.

TERMINE	DESCRIZIONE
Dato Personale	*Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (Art. 4 par. 1 RGPD);*

Trattamento	*Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (Art. 4 par. 2 RGPD);*
Interessato	*La persona fisica alla quale i dati personali si riferiscono (vedasi la definizione di Dato Personale);*
Titolare del trattamento	*La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (Art. 4 par. 7 RGPD). Ai fini della presente Policy il Titolare è la Giunta Regionale del Lazio.*
SDC - Soggetto Designato Competente	*Il Soggetto designato dal Titolare del Trattamento ai sensi degli artt. 474 e 474 ter del RR 1/2002 cui compete il trattamento.*
SDP - Soggetto designato competente in materia di protezione dei dati personali	*Il soggetto designato dal Titolare del Trattamento ai sensi degli artt. 474 e 474 ter del RR 1/2002, competente in materia di protezione dei dati personali.*
DPO (*Data Protection Officer*)	*Soggetto incaricato dal Titolare o dal Responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, di attribuzione di responsabilità e sensibilizzazione, formative e informative relativamente all'applicazione del RGPD (Art. 37 RGPD).*
Principio di protezione dei dati fin dalla progettazione (*privacy by design*)	*Il principio prevede la tutela dei dati personali in fase di progettazione del trattamento attraverso l'adozione di misure tecniche e organizzative adeguate. In tale contesto rilevano parametri quali, la minimizzazione, la pseudonimizzazione dei dati, ovvero tutte le altre misure idonee a ridurre i rischi (Art. 25 par. 1 del RGPD);*
Principio di protezione dei dati per impostazione predefinita (*privacy by default*)	*Il principio prevede, che per impostazione predefinita, il titolare dovrebbe trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. (Art. 25 par. 2 del RGPD);*
Registro dei trattamenti	*Documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.*
***Data protection Impact Assessment* o DPIA (Valutazione d'impatto sulla protezione dei dati)**	*Procedura prevista dall'articolo 35 del RGPD che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un*

	singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. Lo scopo della DPIA è quello di dimostrare che il Titolare abbia messo in atto le misure adeguate nell'esecuzione di un trattamento (Art. 35 RGPD);
Pseudonimizzazione	*Comporta il trattamento dei dati personali in modo tale che gli stessi dati 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 (Art. 4 par. 5 del RGPD);*
Anonimizzazione	*Tecnica che viene applicata ai dati personali in modo tale che le persone fisiche interessate non possano più essere identificate in alcun modo;*
Finalità del trattamento	*Il principio prevede che i dati personali debbano essere "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" (art. 5 par. 1 lett. b) del RGPD).*

Per quanto non espressamente previsto nel presente paragrafo si applicano le definizioni di cui all'art. 4 del RGPD.

5. RIFERIMENTI NORMATIVI

La presente *policy* tiene conto delle seguenti disposizioni nazionali e europee, linee guida e provvedimenti del Garante:

- Regolamento (UE) 2016/679 (di seguito "RGPD");
- D.lgs. 196/2003 (di seguito "Codice in materia di protezione dei dati personali" oppure, per semplicità, "Codice Privacy");
- Linee Guida del Comitato Europeo per la Protezione dei Dati - *European Data Protection Board* "EDPB" - n. 4/2019 concernenti la Data Protection by Design and by Default, ai sensi dell'art. 25 del regolamento 2016/679;
- Linee guida 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, WP 248 rev. 01, 4 ottobre 2017; Provvedimento del Garante "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", 11 ottobre 2018 – Allegato 1.

6. DPIA E PRINCIPIO DI *PRIVACY BY DESIGN E BY DEFAULT*

Ai fini dell'applicazione pratica dei principi di PBDD di cui all'art. 25 del RGPD, l'implementazione di misure tecniche e organizzative che garantiscono l'attuazione dei principi generali, è subordinata ad una valutazione del rischio sulle attività di trattamento da parte del Titolare ai sensi dell'art. 32 RGPD nonché ad una valutazione di impatto (DPIA) ai sensi dell'art. 35 RGPD qualora dagli esiti della valutazione del rischio risulti ancora un rischio elevato per i diritti e le libertà degli interessati.

Il principio della protezione dei dati fin dalla progettazione (*privacy by design*) di cui all'art. 25 par. 1 RGPD, prevede l'obbligo per il Titolare, fin dalla progettazione del trattamento, di prevedere *l'attuazione delle misure tecniche e organizzative adeguate* ai fini della conformità ai principi di protezione dei dati e della tutela dei diritti e delle libertà degli interessati.
In particolare, l'attuazione delle misure tecniche e organizzative deve essere concepita *in funzione dell'efficace attuazione dei principi applicabili al trattamento dei dati personali* di cui all'art. 5 RGPD.
In assenza di un'adeguata applicazione del principio di protezione dei dati sin dalla progettazione il trattamento non può essere effettuato.
Il principio di protezione dei dati per impostazione predefinita (*privacy by default*), di cui all'art. 25, par. 2, del RGPD prevede inoltre che il Titolare attui le misure tecniche e organizzative adeguate a garantire che nelle attività di trattamento siano trattati solo i dati personali necessari e sufficienti alle finalità previste e per il periodo strettamente necessario al raggiungimento di tale finalità.
Anche le soluzioni tecniche adottate dal Titolare devono perseguire di *default* la tutela e la protezione dei dati personali.

7. INDIVIDUAZIONE DEI CRITERI PER L'ESECUZIONE DELLA DPIA

Per ogni nuovo trattamento/progetto/servizio o modifica ad uno già esistente, fin dalle prime fasi della progettazione (*by design*) deve essere effettuata da parte del Titolare una valutazione finalizzata a verificare i potenziali rischi per la sicurezza dei dati tenuto conto dello stato dell'arte e dei costi d'attuazione nonché della natura dei dati (cfr. anche Considerando 83 RGPD).
Si individuano nella tabella che segue i soggetti coinvolti:

R	A	C	I
SDC	SDC	-	-

R=Esecutore A=Responsabile C=Coinvolto I=Informato

Nell'effettuare la valutazione dei rischi di cui all'art. 32 RGPD, il SDC deve considerare in special modo i rischi presentati dal trattamento che derivano da:
- distruzione accidentale o illegale,
- perdita,
- modifica,
- rivelazioni o accesso non autorizzati,
- divulgazione non autorizzata a dati personali trasmessi, conservati o comunque trattati.

Al termine di tale analisi, qualora il trattamento presenti, comunque, un rischio elevato per i diritti e le libertà delle persone fisiche, prima di dare avvio al trattamento compete al SDC l'esecuzione di una DPIA.
Si individuano nella tabella che segue i soggetti coinvolti:

R	A	C	I
SDC	SDC	DPO*	DPO SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

* coinvolgimento eventuale a discrezione del SDC.

Compete al SDC l'esecuzione della DPIA anche qualora il trattamento rientri in uno dei casi contemplati dall'art. 35 Par. 3 del RGPD:
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;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Le casistiche sopra richiamate costituiscono un elenco di alto livello dei criteri che richiedono che il trattamento sia sottoposto ad una valutazione d'impatto, alle quali si aggiungono quelle previste nelle *Linee guida 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*, WP 248 rev. 01 del 4 ottobre 2017, e quelle previste nel Provvedimento del Garante *"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"*, 11 ottobre 2018 – Allegato 1.
Le Linee guida sopra richiamate individuano ulteriori nove criteri utili per l'identificazione dei trattamenti per i quali il Titolare è tenuto a svolgere una DPIA:

1. valutazione o attribuzione di un punteggio all'interessato;
2. trattamenti basati su decisioni automatizzate (es. tracciamento dei comportamenti online);
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
4. trattamento di dati sensibili o dati aventi carattere altamente personale (Artt. 9-10 RGPD);
5. trattamento di dati personali su larga scala;
6. confronto di basi di dati (es. machine learning utilizzato per la trascrizione di parole o il funzionamento di assistenti digitali);
7. trattamento di dati relativi a soggetti vulnerabili (es. minori, migranti, o in genere soggetti che si trovano in condizioni di sudditanza psicologica o di altro tipo rispetto al Titolare);
8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
9. il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Laddove siano presenti almeno due dei criteri succitati il trattamento deve essere oggetto di una DPIA.
È facoltà del SDC anche nel caso in cui un trattamento risponda soltanto ad uno dei criteri sopra richiamati procedere comunque all'esecuzione di una DPIA.
Il Provvedimento del Garante sopra richiamato, ai sensi dell'art. 35 par. 4 del RGPD, prevede un ulteriore elenco di (dodici) tipologie di trattamenti da sottoporre alla valutazione d'impatto:

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;
2. trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato;
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.

4. trattamenti su larga scala di dati aventi carattere estremamente personale: 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);
6. trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, pazienti, richiedenti asilo ecc.);
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 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 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 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 di dati genetici tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Qualora un trattamento rientri in almeno una delle tipologie previste nel Provvedimento del Garante il trattamento stesso deve essere oggetto di una DPIA.

Il SDC, quando il trattamento presenta le caratteristiche di seguito indicate può non procedere all'esecuzione della DPIA:

- il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati;
- le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10);
- il trattamento è incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5) qualora adottato dal Garante nazionale.

Ai sensi dell'art. 474 ter il SDC all'esito della DPIA, laddove ritenga opportuno richiedere il parere di cui all'art. 474 septies del Regolamento regionale, trasmette la stessa al DPO.

8. CONTENUTI OBBLIGATORI DELLA DPIA

Tenuto conto di quanto stabilito all'art 35 par. 7 RGPD, si definiscono di seguito i contenuti obbligatori della valutazione di impatto:

- una descrizione sistematica del trattamento;
- una valutazione della necessità e della proporzionalità del trattamento in cui sono esplicitate e giustificate le modalità con cui viene garantita la liceità del trattamento, in termini di:
- indicazione delle finalità: devono essere definite le finalità specificate esplicite e legittime;
- minimizzazione dei dati: deve essere limitata la quantità dei dati personali trattati a ciò che risulti strettamente necessario ai fini dell'esecuzione del trattamento;
- limitazione della conservazione: deve essere definito il periodo di conservazione necessario per raggiungere le finalità indicate.
- l'indicazione delle misure previste per affrontare i rischi incluse le garanzie per assicurare la protezione dei dati personali e la dimostrazione della conformità al RGPD tenuto conto anche delle modalità di gestione dei diritti dell'interessato.

Nel rispetto del principio di PBDD, il Titolare del trattamento procede a un riesame periodico del trattamento dei dati personali al fine di valutare che lo stesso sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati. È fatto comunque obbligo al Titolare di procedere all'aggiornamento della DPIA ogniqualvolta insorgono variazioni del rischio delle attività di trattamento.

9. DPIA SU PRODOTTI/SERVIZI CON L'USO DI NUOVE TECNOLOGIE.

L'obbligo di svolgere la valutazione d'impatto (DPIA) è in capo al Titolare del trattamento; tuttavia, nel caso in cui la Giunta Regionale del Lazio, nel suo ruolo *privacy* di Titolare, stabilisca che il trattamento sia effettuato per suo conto da un fornitore di servizi, prodotti e applicazioni, Responsabile del trattamento, potrà richiedere di essere assistito da quest'ultimo in conformità al relativo contratto sottoscritto tra le parti e nel rispetto specifico dell'art. 28, par. 3, lett. f), del RGPD.

Qualora il trattamento preveda l'utilizzo di servizi e prodotti con l'uso di nuove tecnologie da parte di Fornitori-Responsabili del trattamento è necessario che il Titolare, fermo l'obbligo dello stesso di svolgere una propria specifica DPIA, acquisisca dal fornitore, quale requisito di accesso alla fase di selezione del contraente, una valutazione di impatto sulla protezione dei dati sul prodotto/servizio da acquistare.

10. CONSULTAZIONE PREVENTIVA CON L'AUTORITÀ GARANTE

Nel caso in cui la Valutazione d'impatto evidenzi un "Rischio elevato residuale", il Soggetto Designato competente (SDC), qualora intenda comunque procedere al trattamento, sentito il DPO, avvia la Consultazione Preventiva con l'Autorità di controllo ai sensi dell'art 36 par. 1 del RGPD.

Si individuano nella tabella che segue i soggetti coinvolti:

R	A	C	I
SDC	SDC	DPO	DPO SDP

R=Esecutore A=Responsabile C=Coinvolto I=Informato

È competenza del SDC, sentito il DPO, redigere l'istanza di consultazione preventiva ai sensi dell'art. 36 par. 3 del RGPD, contenente i seguenti elementi:

- le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del RGPD;
- i dati di contatto del responsabile della protezione dei dati (DPO);
- la valutazione d'impatto sulla protezione dei dati (DPIA) effettuata;
- ogni altra informazione richiesta dall'Autorità di controllo.

L'art. 36, par. 2, del RGPD stabilisce che l'Autorità di controllo, se ritiene che il trattamento previsto non sia conforme al RGPD o che il Titolare non abbia identificato o attenuato sufficientemente il rischio, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce un parere scritto. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il Titolare e, ove applicabile, il responsabile del trattamento ne sono informati unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta. Tali periodi possono essere sospesi fino all'ottenimento da parte dell'Autorità di controllo delle informazioni eventualmente richieste ai fini della consultazione.

È inoltre prevista la consultazione del Garante nella casistica dell'art. 36 par. 4 RGPD o nel caso in cui la normativa prescriva che il titolare del trattamento consulti l'autorità di controllo, e ne ottenga l'autorizzazione preliminare, in relazione al trattamento per l'esecuzione di un compito di interesse pubblico, tra cui rientrano i trattamenti con riguardo alla protezione sociale e alla sanità pubblica (art. 36 par. 4 RGPD).

All'esito della valutazione da parte dell'Autorità Garante e della trasmissione del parere scritto nei termini di cui al par. 2 dell'art. 36 del RGPD, il SDC coadiuvato dal DPO, individua e mette in atto le misure e le azioni necessarie per l'adeguamento alle prescrizioni impartite.