ALLEGATO PP ([1])

PRIVACY BY DESIGN & BY DEFAULT POLICY

- versione 1.0 -

[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.

1. INTRODUZIONE

La presente *policy* descrive i principi di *privacy by design e by default* e fornisce indicazioni per la sua applicazione pratica e per la conduzione del processo di *Data Protection by Design-by Default*. La *policy* si applica a tutte le attività di trattamento poste in essere dalla Giunta Regionale in qualità di Titolare del trattamento anche per il tramite di Responsabili/Sub-responsabili del trattamento individuati ai sensi dell'art. 28 del RGPD relativamente alle funzioni e alle competenze dell'Ente.

1.1 Glossario

Ai fini della presente *policy* si intende per:

- **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):*
- **raccolta**: attività di acquisizione del dato;
- **registrazione**: memorizzazione dei dati su un qualsiasi supporto;
- **organizzazione**: classificazione dei dati secondo un metodo prescelto;
- **strutturazione**: attività di distribuzione dei dati secondo schemi precisi;
- **conservazione**: mantenere le informazioni su un qualsiasi supporto;
- **elaborazione**: attività con la quale il dato personale subisce una modifica sostanziale (la modificazione può riguardare anche solo parte minima del dato personale);
- **estrazione**: attività di estrapolazione di dati da gruppi già memorizzati;
- **consultazione**: lettura dei dati personali (anche la semplice visualizzazione);
- **uso**: attività generica che ricopre qualsiasi tipo di impiego di dati;
- **comunicazione**: dare conoscenza di dati personali ad uno o più soggetti diversi dall'interessato, dal responsabile o dagli autorizzati (dato trasferito a terzi), comunque in numero determinato;
- d**iffusione** si intende invece il dare conoscenza a soggetti indeterminati, in qualunque forma;
- **raffronto**: operazione di confronto tra dati, sia in conseguenza di elaborazione che di consultazione;
- **interconnessione**: utilizzo di più banche dati;
- **limitazione**: conservazione con sospensione temporanea di ogni altra operazione di trattamento;
- **cancellazione**: eliminazione di dati tramite utilizzo di strumenti elettronici;
- **distruzione**: attività di eliminazione definitiva dei dati.
- **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 RGDP).

- **Responsabile del trattamento**: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (Art. 28 RGPD).*
- **Destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi (*Art. 4, par. 1, n. 9 del RGDP*).
- **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.*
- **Principio di responsabilizzazione (*accountability*):** *adozione di comportamenti proattivi da parte del Titolare o del Responsabile del trattamento, tali da dimostrare e documentare la concreta adozione di misure finalizzate ad assicurare l'applicazione del RGPD alle attività di trattamento.*
- **Minaccia**: *identifica una situazione di "pericolo" la cui realizzazione potrebbe incidere sulla riservatezza, e/o integrità, e/o disponibilità dei dati e sui diritti e le libertà degli interessati.*
- **Probabilità***: corrisponde alla possibilità di realizzazione di una minaccia.*
- **Impatto:** *corrisponde alle conseguenze negative sui diritti e le libertà degli interessati nel caso in cui si concretizzi la minaccia.*
- **Valutazione del rischio***: è il processo di valutazione che analizza lo scenario del rischio in relazione alla probabilità combinata con i possibili impatti negativi sulle libertà e i diritti degli interessati tenendo conto delle misure tecniche e organizzative che il Titolare ha adottato o intende adottare per mitigare il rischio stesso.*
- **Rischio inerente:** *è determinato dal valore del rischio in relazione alla probabilità di accadimento della minaccia e dell'impatto al concretizzarsi della stessa in assenza di misure di mitigazione.*
- **Rischio residuo:** *è determinato dal valore del rischio dopo l'applicazione da parte del Titolare delle misure tecniche e organizzative finalizzate alla mitigazione del rischio inerente.*
- **DPIA:** è *la valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessments) da effettuare ogniqualvolta, all'esito della valutazione del rischio, il trattamento dei dati continua a comportare un rischio residuo elevato per i diritti e le libertà degli interessati e in tutti gli altri casi previsti dall'articolo 35 del RGPD.*

Per quanto non espressamente previsto nel presente paragrafo si applicano le definizioni contenute nel RGPD.

1.2 Premessa

Il rispetto dei principi di protezione dei dati fin dalla progettazione (*privacy by design*) e di protezione per impostazione predefinita (*privacy by default*) stabilito dall'articolo 25 del RGPD costituisce un obbligo per il Titolare del trattamento che è chiamato a predisporre le misure adeguate e le garanzie finalizzate ad una attuazione efficace dei principi del trattamento dei dati nonché alla massima protezione dei diritti e delle libertà degli interessati.
Il Titolare deve applicare i principi di *privacy by design e by default:*

- prima di iniziare una nuova attività di trattamento e sin dalla progettazione della stessa;

- durante lo svolgimento dell'attività di trattamento verificando costantemente l'efficacia delle misure adottate e delle garanzie individuate.

  L'applicazione dei principi di *privacy by design e by default* si riferisce anche alle attività di trattamento nell'ambito di sistemi preesistenti, anche ante RGPD.

  Inoltre, la presente policy deve essere presa sistematicamente in considerazione nell'ambito degli appalti pubblici: la Regione è tenuta ad assicurare il rispetto degli obblighi di *privacy by design e by default* in relazione al trattamento svolto dai rispettivi responsabili e sub-responsabili e, pertanto, deve tenerne conto quando stipula contratti con tali soggetti.

  La presente *policy*, tenuto conto del contesto specifico del trattamento, esamina gli elementi chiave della progettazione (*by design*) e dell'impostazione predefinita (*by default*) e la loro applicazione pratica, al fine di fornire indicazioni per un'efficace attuazione dei principi di protezione dei dati contenuti nell'articolo 5 del RGPD.

  In attuazione di tali principi, il Titolare del trattamento, anche quando utilizza sistemi tecnologici realizzati da terzi, deve eseguire un'analisi dei rischi ed eventualmente una valutazione d'impatto e accertarsi che le funzionalità corrispondano alle finalità del trattamento individuate che abbiano una specifica base giuridica.

1.3 Scopo

Lo scopo della presente *policy* è quello di fornire indicazioni volte ad applicare i principi di *privacy by design & by default* nelle fasi di definizione e di attuazione di un processo[2] nel caso in cui lo stesso contempli l'uso di dati personali, in modo che il Titolare possa essere in grado di dimostrare e documentare che le proprie attività siano assistite da misure di sicurezza e garanzie adeguate ad assicurare il rispetto dei principi di protezione dei dati e la tutela dei diritti e delle libertà degli interessati.

2. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (*privacy by design*) E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (*privacy by default)*

2.1 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE - *PRIVACY BY DESIGN* (ART. 25 PAR. 1 RGPD)

L'obbligo del rispetto del principio della protezione dati fin dalla progettazione (*privacy by design*) consiste nell'obbligo del Titolare del trattamento di attuare le misure tecniche e organizzative adeguate[3] e le necessarie garanzie a tutela dei diritti e delle libertà degli interessati prima che inizi qualunque attività di trattamento.

Le misure tecniche e organizzative adottate dal Titolare devono essere:

[2] Si intende per processo l'insieme di operazioni/azioni, poste in essere da soggetti o strutture organizzative finalizzate al raggiungimento di uno specifico scopo. Rientrano nel concetto di processo riferito alle attività e alle funzioni della Giunta Regionale, a titolo esemplificativo e non esaustivo: le proposte di leggi regionali, i regolamenti, gli atti amministrativi generali, gli atti di organizzazione, i bandi di concorso e le procedure di reclutamento, i bandi di gara e i contratti pubblici, l'erogazione di contributi, le campagne di comunicazione e informazione, lo sviluppo e la gestione di sistemi informativi, ecc.

[3] Le misure adottate dal Titolare, tenuto conto del contesto del trattamento, possono comprendere, a titolo esemplificativo e non esaustivo: la pseudonimizzazione dei dati personali, la memorizzazione di dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, la possibilità per gli interessati di intervenire nel trattamento, l'informazione sulla conservazione dei dati personali, la disponibilità di sistemi di rilevamento di malware, la formazione dei dipendenti, l'istituzione di sistemi di gestione della privacy e della sicurezza delle informazioni, l'obbligo contrattuale per i responsabili del trattamento di attuare prassi specifiche di minimizzazione dei dati, adozione di standard, migliori prassi e codici di condotta riconosciuti da associazioni e da altri organismi.

- adeguate: funzionali all'attuazione dei principi del trattamento di cui all'art. 5 del RGPD e della conseguente tutela dei diritti degli interessati;
- efficaci:
  - perseguire i risultati previsti dal Titolare;
  - individuate in relazione allo specifico trattamento e in rapporto alla valutazione dei rischi dello stesso;
  - definite all'esito della valutazione degli elementi di cui al paragrafo che segue;
- documentate e dimostrabili: il Titolare del trattamento deve disporre della documentazione relativa alle misure tecniche e organizzative applicate dalla quale si evinca la dimostrazione dell'efficacia delle misure stesse (ad esempio attraverso l'uso di indicatori di efficacia[4]).

2.1.1 Elementi da valutare nella determinazione delle misure

Il Titolare, quando determina le misure tecniche e organizzative relative ad uno specifico trattamento deve tenere conto, dei seguenti elementi:

a. stato dell'arte;
b. costi di attuazione;
c. natura, ambito di applicazione, contesto e finalità del trattamento;
d. rischi per i diritti e le libertà degli interessati dal trattamento;
e. fattore temporale.

a. Stato dell'arte

La valutazione di questo elemento è applicabile sia alla determinazione delle misure tecniche che alla determinazione di quelle organizzative integrate nel trattamento.

La valutazione dello stato dell'arte nella determinazione delle misure tecniche consiste prevalentemente nelle seguenti attività del Titolare del Trattamento:

- valutazione dello stato della tecnologia applicata allo specifico trattamento disponibile sul mercato;
- valutazione dei rischi che la tecnologia applicata determina sul trattamento;
- valutazione dello stato delle misure e delle garanzie disponibili ed efficaci in rapporto all'evoluzione del panorama tecnologico.

La valutazione dello stato dell'arte nella determinazione delle misure organizzative consiste prevalentemente nelle seguenti attività del Titolare del Trattamento:

- valutazione delle politiche interne adottate ed eventualmente della necessità del loro adeguamento;
- valutazione del livello della formazione del personale con particolare riferimento al contesto tecnologico;
- valutazione delle politiche di gestione e di governance della sicurezza informatica.

Nelle valutazioni sopra richiamate il Titolare può:

- prendere a riferimento standard, certificazioni e/o codici di condotta esistenti e riconosciuti che possono contribuire a indicare lo "stato dell'arte" nello specifico ambito;

[4] Gli indicatori possono essere quantitativi (es. riduzione di reclami e/o segnalazioni, diminuzione dei tempi di risposta alle istanze dei diritti degli interessati, ecc) o qualitativi (es. valutazioni delle prestazioni, ecc.).

- utilizzare i livelli di protezione previsti negli standard sopra richiamati ai fini della progettazione e dell'attuazione delle misure di protezione dei dati.
  Lo stato dell'arte è un concetto dinamico, soggetto ad una valutazione continua, soprattutto se riferito al contesto tecnologico; pertanto, il Titolare è tenuto a periodiche valutazioni finalizzate alla verifica che le misure individuate garantiscano un livello di protezione adeguato e provvedere, all'occorrenza al loro aggiornamento; una condotta difforme determina la mancata osservanza dell'articolo 25 del RGPD.

b. Costi di attuazione

La valutazione di questo elemento è applicabile sia alla determinazione delle misure tecniche che alla determinazione di quelle organizzative integrate nel trattamento. Il concetto di "costo di attuazione" ha una accezione ampia e contempla la valutazione delle risorse legate a diversi fattori: tempo, risorse umane, dotazioni strutturali, risorse economiche, ecc.

La valutazione del "costo di attuazione" nella determinazione delle misure tecniche e organizzative consiste prevalentemente nelle seguenti attività del Titolare del Trattamento:

- valutazione dell'economicità intesa come impiego di quantità di risorse proporzionata all'efficacia al fine di evitare soluzioni eccessivamente dispendiose e di adottare, in caso di efficacia equivalente, soluzioni più economiche;
- gestione dei costi complessivi come sopra determinati al fine di attuare con efficacia i principi di protezione dati e la tutela dei diritti degli interessati.
  Il Titolare, per non incorrere nella mancata osservanza dell'articolo 25 del RGPD, è comunque tenuto ad assicurarsi che, indipendentemente dal costo, le misure individuate garantiscano che l'attività di trattamento sia conforme ai principi di cui all'art. 5 del RGPD.

c. Natura, ambito di applicazione, contesto e finalità del trattamento

La valutazione di questi elementi è applicabile sia nella determinazione delle misure tecniche che nella determinazione di quelle organizzative integrate nel trattamento. Allo scopo di integrare principi di protezione dei dati nella progettazione del trattamento, questi fattori devono essere interpretati in coerenza con altre disposizioni del RGPD, tra cui gli artt. 24, 32 e 35.

L'analisi di questi fattori nella determinazione delle misure consiste nelle seguenti attività del Titolare del Trattamento riferite al singolo fattore:

- natura: valutazione delle caratteristiche intrinseche del trattamento;
- ambito di applicazione: valutazione della dimensione e dell'ampiezza del trattamento;
- contesto: valutazione delle circostanze che possono influenzare le aspettative degli interessati dal trattamento;
- finalità: determinazione degli obiettivi del trattamento.

d. Rischi per i diritti e le libertà degli interessati dal trattamento

Al fine di individuare le misure tecniche e organizzative adeguate alla tutela delle persone fisiche e dei loro dati personali e di adempiere ai requisiti previsti dal RGPD, il Titolare del trattamento, nel determinare le misure tecniche e organizzative adotta un approccio basato sul rischio (artt. 24, 25, 32 e 35 RGPD).

La valutazione del rischio per la sicurezza dei dati - e del trattamento - nella determinazione delle misure tecniche e organizzative consiste in un esame sistematico e approfondito del trattamento e determina le seguenti attività in capo al Titolare del Trattamento:

- individuazione dei rischi inerenti presentati dal trattamento dei dati personali;
- determinazione della probabilità di accadimento della minaccia e dell'impatto della stessa sui diritti degli interessati;
- individuazione di misure efficaci a mitigare il rischio individuato;
- valutazione del rischio residuo;
- esecuzione di una DPIA qualora il trattamento dei dati continui a comportare un rischio residuo elevato per i diritti e le libertà degli interessati.

  Il Titolare nella valutazione dei rischi del trattamento, al fine di affrontare rischi simili in situazioni analoghe (natura, ambito di applicazione, contesto e finalità del trattamento) può utilizzare anche dati di riferimento derivanti dalle migliori prassi e/o standard, ma anche in questo caso è comunque chiamato a:

- effettuare una valutazione del rischio per la sicurezza dei dati e del trattamento per ogni attività di trattamento;
- verificare l'efficacia delle misure adottate e delle garanzie proposte;
- valutare se il trattamento necessita di una valutazione d'impatto (DPIA) ex art. 35 RGPD;
- aggiornare periodicamente la valutazione del rischio e la valutazione di impatto e verificare la conformità del trattamento.

e. Fattore temporale

Il Titolare del trattamento deve integrare i principi di protezione dei dati nella progettazione del trattamento in fase precoce, sin dal *"momento di determinare i mezzi del trattamento";* i *"mezzi del trattamento"* rappresentano gli elementi generali della progettazione di un trattamento, e individuano come effettuare il trattamento stesso e i meccanismi impiegati per attuarlo.

L'applicazione del fattore temporale impone al Titolare, al momento di definire l'architettura, la procedura e i protocolli applicabili al trattamento, di mettere in atto le seguenti attività:

- valutazione delle misure e delle garanzie adeguate ad attuare efficacemente i principi e tutelare i diritti degli interessati;
- valutazione dei rischi e di tutti gli altri elementi che concorrono all'applicazione concreta del principio di privacy *by design* sopra analizzati (stato dell'arte, costo di attuazione, natura del trattamento, ambito di applicazione, contesto e finalità);
- valutazione dei tempi e dei costi/benefici dei servizi necessari al trattamento dati *ex ante* (es. software e hardware), in modo da scongiurare modifiche successive su trattamenti già progettati, pianificati e definiti.

2.1.2 Mantenimento e verifica dei requisiti in materia di protezione dei dati e sistemi preesistenti

Una volta avviato il trattamento, al fine di dare un'attuazione efficace e costante ai principi nonché di tutelare i diritti, il Titolare è tenuto a mantenere su base continuativa l'applicazione dei principi di *privacy by design e by default.* L'ambito di applicazione, il contesto delle operazioni di trattamento, nonché il rischio possono mutare nel corso del trattamento; pertanto, è fatto obbligo al Titolare di verificare e riesaminare periodicamente l'efficacia delle misure e delle garanzie poste in essere.

Tale obbligo si applica anche:

- ai sistemi preesistenti: i sistemi progettati prima dell'entrata in vigore del RGPD devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie adeguate ed efficaci;
- ai trattamenti svolti per mezzo di Responsabili del trattamento: le operazioni di trattamento effettuate dai Responsabili devono essere regolarmente esaminate e valutate, almeno annualmente, dal Titolare per garantire che continuino a rispettare i principi e permettano ai Titolari stessi di adempiere agli obblighi in materia di protezione dei dati personali.

2.2 PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA - *PRIVACY BY DEFAULT* (ART. 25 PAR. 2 RGPD)

L'espressione *privacy by default* (per impostazione predefinita) si riferisce all'obbligo del Titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. L'impostazione predefinita si riferisce alle scelte compiute rispetto a valori di configurazione od opzioni di trattamento (esempio un'applicazione informatica, un servizio ecc.), tali da incidere sulla quantità dei dati personali raccolti, sulla portata del trattamento, sul periodo di conservazione e sull'accesso ai dati.

Ai fini dell'applicazione del principio di *privacy by default* (per impostazione predefinita) il Titolare deve:

- trattare solo dati personali necessari per ogni specifica finalità del trattamento:
  Il Titolare, dopo aver valutato la necessità del trattamento in relazione alle condizioni di liceità previste dal RGPD, deve impostare le attività di trattamento in modo da garantire che venga effettuato solo il trattamento di dati strettamente necessari per conseguire la specifica e lecita finalità dello stesso e conservarli per il periodo strettamente necessario, a tal fine è tenuto:

- a definire in anticipo quali dati personali debbano essere raccolti e trattati per le finalità specifiche, esplicite e legittime dello specifico trattamento;
- a definire, per impostazione predefinita, le misure che garantiscano il trattamento dei soli dati personali necessari;
- ad eseguire, in caso di utilizzo di software di terze parti, una valutazione dei rischi del prodotto ed a disattivare, all'occorrenza, funzioni che non hanno una base giuridica o che non sono compatibili con le finalità del trattamento.
- tenere conto del perimetro dell'obbligo di minimizzazione dei dati di cui all'art. 25, paragrafo 2, RGPD che vale per:
- la quantità dei dati personali raccolti: le impostazioni predefinite non devono includere la raccolta di dati personali che non siano necessari per la specifica finalità del trattamento; tale impostazione prescrive di non raccogliere dati in eccesso rispetto a quelli strettamente necessari, ma anche di non raccogliere dati particolareggiati qualora dati meno granulari siano sufficienti al raggiungimento delle finalità del trattamento;
- la portata del trattamento: le impostazioni predefinite devono garantire che i trattamenti effettuati sui dati personali si limitano alle operazioni strettamente necessarie al raggiungimento delle finalità;
- il periodo di conservazione: le impostazioni predefinite devono garantire che il periodo di conservazione dei dati personali corrisponda al tempo strettamente necessario al raggiungimento della specifica finalità del trattamento. La scelta del tempo di conservazione, in base al principio di responsabilizzazione, deve essere giustificabile e documentabile da parte del Titolare.
- l'accesso ai dati: le impostazioni predefinite devono limitare il più possibile l'accesso ai dati, pertanto il Titolare deve:

- limitare l'accesso ai dati personali esclusivamente a soggetti autorizzati;
- abilitare gli accessi ai dati personali solo dopo la valutazione sull'effettiva necessità del trattamento degli stessi; i dati devono essere resi accessibili a un numero definito di persone fisiche;
- effettuare i controlli sugli accessi per l'intero flusso dei dati per la durata del trattamento.

3. *PRIVACY BY DESIGN E BY DEFAULT* NELL'ATTUAZIONE DEI PRINCIPI DI PROTEZIONE DATI

Il Titolare deve tenere in considerazione gli elementi e i fattori della *privacy by design e by default* richiamati nei paragrafi che precedono in tutte le fasi di progettazione delle attività di trattamento, anche nell'attuazione dei principi di protezione dati indicati nell'articolo 5 e nel considerando 39 del RGPD:

3.1 trasparenza;
3.2 liceità;
3.3 correttezza;
3.4 limitazione delle finalità;
3.5 minimizzazione dei dati;
3.6 esattezza;
3.7 limitazione della conservazione;
3.8 integrità e riservatezza;
3.9 responsabilizzazione.

3.1 Trasparenza

Il principio di trasparenza del trattamento è rinvenibile negli articoli 12, 13, 14 e 34 del RGPD. Il Titolare ha l'obbligo di effettuare attività di trattamento trasparenti al fine di consentire agli interessati di comprendere il trattamento dei dati che li riguardano e, all'occorrenza, di avvalersi dei diritti di cui agli artt. 15 e ss del RGPD.

L'applicazione del principio della trasparenza nella *privacy by design e by default* impone al Titolare che le informazioni agli interessati abbiano le seguenti caratteristiche:

- chiarezza – linguaggio chiaro, semplice, conciso, comprensibile;
- accessibilità – facilità di accesso per gli interessati;
- contestualità – fornite al momento opportuno e nella forma adeguata;
- pertinenza – pertinenti e applicabili all'interessato specifico;
- progettazione universale – rispondere a criteri di accessibilità per tutti gli interessati anche utilizzando linguaggi leggibili da macchine che agevolino e/o automatizzino la leggibilità;
- comprensibilità – gli interessati devono avere una buona comprensione di ciò che possono aspettarsi dal trattamento dei loro dati personali, in particolare quando si tratti di minori o di soggetti appartenenti ad altre categorie vulnerabili;
- multicanalità – devono essere fornite attraverso canali e mezzi di comunicazione diversi per aumentare la probabilità che raggiungano efficacemente l'interessato;
- approccio multilivello – devono essere fornite secondo un approccio multilivello, con l'evidenziazione dei punti più importanti e rendendo facilmente accessibili informazioni più dettagliate con collegamenti a ulteriori punti e concetti (es. attraverso menu a discesa) al fine di garantire un equilibrio tra completezza e comprensibilità.

3.2 Liceità

Il Titolare ha l'obbligo di identificare una base giuridica valida per il trattamento dei dati personali di sua competenza e l'intero ciclo di vita del trattamento deve essere in linea con la base giuridica identificata.

Gli elementi da valutare ai fini del principio di liceità nell'applicazione della *privacy by design e by default* sono:

- pertinenza: il trattamento deve essere riferito a una corretta base giuridica;
- differenziazione: la base giuridica va differenziata e riferita a ciascuna specifica attività di trattamento;
- specificità della finalità: la base giuridica deve essere connessa alla specifica finalità di trattamento;
- necessità: il trattamento deve essere necessario e non soggetto a condizioni affinché la sua finalità sia lecita;
- consenso: il consenso deve essere liberamente espresso, specifico, informato e inequivocabile. Quando il Titolare del trattamento è una pubblica autorità, il consenso costituisce una base giuridica residuale e non dovrebbe potersi considerare un valido fondamento giuridico a causa dello squilibrio tra l'interessato e il Titolare;
- revoca del consenso: qualora la base giuridica del trattamento si identifichi con il consenso per la revoca dello stesso deve essere garantita con la stessa facilità con cui è stato prestato;
- bilanciamento degli interessi: quando la base giuridica è costituita da interessi legittimi, il Titolare deve effettuare un bilanciamento ponderato, considerando in particolare lo squilibrio tra i rapporti di forza, (in particolare in caso di minori o soggetti vulnerabili) e devono essere previste misure e garanzie per attenuare l'impatto negativo sugli interessati. La condizione del legittimo interesse non si applica al trattamento di dati effettuato dalle pubbliche autorità;
- predeterminazione: la base giuridica è stabilita prima di iniziare l'attività di trattamento;
- cessazione; in presenza di una base giuridica non valida il trattamento va immediatamente cessato;
- attribuzione di responsabilità; in caso di contitolarità del trattamento, le parti individuano in modo chiaro e trasparente le basi giuridiche ed elaborano le misure del trattamento in relazione alle stesse.

3.3 Correttezza

La correttezza è un principio di natura trasversale che impone di non trattare i dati in modo dannoso, discriminatorio, imprevisto o fuorviante per l'interessato. Il principio di correttezza integra i diritti e le libertà degli interessati con particolare riferimento al diritto di essere informati (trasparenza), al diritto di intervenire nel trattamento (accesso, cancellazione, portabilità dei dati, rettificazione) e al diritto di limitazione del trattamento, nonché il diritto a non essere sottoposto a un processo decisionale automatizzato e non subire discriminazioni nel contesto di tali processi; il diritto alla portabilità dei dati, ai sensi dell'art. 20, par. 3, del RGPD, non si applica al trattamento effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Gli elementi da valutare ai fini del principio di correttezza nell'applicazione della *privacy by design e by default* sono:

- interazione: garantire agli interessati l'esercizio dei propri diritti in relazione ai dati personali trattati dal Titolare;
- aspettativa; il trattamento deve corrispondere alle aspettative ragionevoli degli interessati;
- assenza di discriminazione: dal trattamento non deve derivare alcuna discriminazione degli interessati;

- assenza di sfruttamento: il trattamento non deve generare sfruttamento delle vulnerabilità degli interessati;
- rispetto dei diritti: il trattamento deve rispettare i diritti fondamentali degli interessati; eventuali compressioni degli stessi devono essere espressamente previste dalla legge;
- eticità: il trattamento deve essere effettuato nel rispetto dei diritti e della dignità delle persone;
- veridicità: il trattamento deve essere effettuato secondo le modalità comunicate agli interessati.

3.4 Limitazione delle finalità

Il principio della limitazione delle finalità impone al Titolare di raccogliere e trattare dati per finalità specifiche, esplicite e legittime e di non trattarli ulteriormente oltre i limiti delle finalità definite.

Il trattamento in fase di progettazione deve essere sviluppato per conseguire le finalità definite; in caso di trattamento ulteriore, il Titolare ha l'obbligo di verificare periodicamente se lo stesso sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti tenendo conto dei seguenti elementi:

- nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
- natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
- possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Gli elementi da valutare ai fini del principio di limitazione delle finalità nell'applicazione della *privacy by design e by default* sono:

- predeterminazione: le finalità sono determinate prima della progettazione del trattamento;
- specificità: le finalità sono specifiche ed esplicite e si riferiscono al motivo per cui i dati personali vengono trattati;
- orientamento in base alla finalità: le finalità orientano la progettazione del trattamento e ne determinano i limiti;
- necessità: la finalità determina quali sono i dati personali necessari per il trattamento;
- compatibilità: eventuali nuove finalità determinano una verifica della compatibilità con la finalità originaria per la quale i dati sono stati raccolti e, ove necessario, modifiche nella progettazione del trattamento;
- limitazione di trattamenti ulteriori: non devono essere effettuati ulteriori trattamenti per finalità diverse che non sono compatibili con quelle originariamente determinate;
- limitazioni del riutilizzo; il Titolare ha l'obbligo di limitare la possibilità di riutilizzo dei dati personali adottando adeguate misure tecniche (es. hashing e/o cifratura) e organizzative (es. politicy, definizione di clausole e obblighi contrattuali);
- riesame periodico: il Titolare ha l'obbligo di verificare periodicamente se il trattamento sia necessario per le finalità per le quali sono stati raccolti i dati e testare la progettazione di tale trattamento con riguardo al principio di limitazione delle finalità.

3.5 Minimizzazione dei dati

Il Titolare può sottoporre a trattamento solo i dati che risultino adeguati, pertinenti e limitati al perseguimento della finalità cui sono sottoposti. Il principio di minimizzazione dei dati obbliga

il Titolare, prima di iniziare il trattamento e durante il ciclo di vita dello stesso, ad effettuare le seguenti valutazioni:

- se per le finalità individuate sia necessario trattare i dati personali;
- se sia possibile conseguire ugualmente le finalità individuate trattando una quantità inferiore di dati personali o utilizzando dati meno dettagliati o aggregati;
- se le finalità individuate possano essere conseguite con un minor grado di identificazione dei dati:
- verificare se la finalità sia perseguibile anche con dati statistici e aggregati non riferiti a persone fisiche identificate o identificabili;
- verificare se i dati riferiti alle persone fisiche originariamente necessari per il trattamento iniziale siano ancora necessari;
- cancellare o rendere anonimi i dati personali nel caso in cui non sia più necessaria l'identificazione;
- pseudonimizzare i dati nel caso in cui l'identificazione continui ad essere necessaria per le altre attività di trattamento al fine di ridurre i rischi per i diritti degli interessati.

Gli elementi da valutare ai fini del principio di minimizzazione dei dati nell'applicazione della *privacy by design e by default* sono:

- evitare il trattamento dei dati qualora la finalità sia comunque raggiungibile anche senza di esso;
- limitazione: limitare la quantità di dati personali raccolti a ciò che è necessario per la specifica finalità;
- limitazione dell'accesso: limitare al minimo il numero di persone che accede ai dati personali per esercitare le proprie funzioni;
- pertinenza: limitare l'utilizzo dei dati personali a quelli pertinenti al trattamento; dimostrare tale pertinenza;
- necessità: limitare il trattamento ai dati senza i quali non è possibile conseguire la specifica finalità;
- aggregazione: prediligere ove possibile l'utilizzo di dati aggregati;
- pseudonimizzazione: pseudonimizzare i dati personali quando non è più necessario disporre di dati personali identificabili e memorizzare le chiavi di identificazione separatamente;
- anonimizzazione e cancellazione: rendere anonimi e cancellare tutti i dati personali che non sono più necessari per la specifica finalità;
- flusso dei dati: il flusso dei dati non deve generare copie ulteriori di dati rispetto a quanto necessario alle finalità del trattamento;
- stato dell'arte: applicare tecnologie aggiornate e adeguate a minimizzare il trattamento dei dati.

3.6 Esattezza

Il Titolare ha l'obbligo di adottare adeguate misure tecniche e organizzative per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati affinché i dati personali utilizzati siano esatti e, se necessario, aggiornati. La valutazione del requisito dell'esattezza del dato va effettuata anche in relazione al rischio concreto derivante dall'utilizzo di dati inesatti[5].

Gli elementi da valutare ai fini del principio di esattezza dei dati nell'applicazione della *privacy by design e by default* sono:

- fonte dei dati: utilizzare solo fonti di dati personali attendibili;

[5] Si riportano di seguito alcuni esempi di conseguenze derivanti dal trattamento di dati inesatti: diagnosi errate, applicazione di errati protocollo sanitari, decisioni erronee conseguenti a processi manuali o automatizzati ecc.

- grado di esattezza: ciascun elemento di dato personale deve essere il più esatto possibile in base alle specifiche finalità individuate;
- esattezza misurabile: utilizzare sistemi e applicare misure che riducano al minimo numero di falsi positivi/negativi;
- verifica: verificare la correttezza dei dati personali presso l'interessato prima del trattamento e nelle sue diverse fasi a seconda della natura dei dati, e in relazione alla frequenza delle relative modifiche;
- cancellazione/rettifica: cancellare o rettificare tempestivamente i dati inesatti;
- evitare/limitare la propagazione di errori: al verificarsi dell'errore attenuarne l'effetto nella catena di trattamento;
- accesso: fornire agli interessati adeguate e pertinenti informazioni in modo che gli stessi, all'occorrenza, possano efficacemente esercitare i diritti di cui agli artt. 15 e ss. del RGPD;
- esattezza permanente; assicurare l'esattezza dei dati in tutte le fasi del trattamento ed effettuare verifiche di esattezza nelle fasi critiche;
- aggiornamento: aggiornare i dati personali ogni qualvolta si renda necessario per il raggiungimento della specifica finalità;
- progettazione dei dati: adottare misure organizzative e tecniche di progettazione finalizzate alla limitazione delle inesattezze dei dati (es. limitazione dei campi a testo libero predisponendo la possibilità di scelte predeterminate).

3.7 Limitazione della conservazione

I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un periodo limitato a quello necessario per le finalità per le quali i dati personali sono trattati. La finalità del trattamento è il criterio principale per stabilire la durata della conservazione dei dati personali.

Gli elementi da valutare ai fini del principio di limitazione della conservazione dei dati nell'applicazione della *privacy by design e by default* sono:

- periodo di conservazione: il periodo di conservazione deve essere riferito alla specifica finalità del trattamento individuata.
- cancellazione e anonimizzazione: predisporre procedure interne per la cancellazione e/o l'anonimizzazione dei dati; l'anonimizzazione può costituire un'alternativa alla cancellazione, a condizione che siano valutati la probabilità e la gravità del rischio ivi compreso quello della eventuale re-identificazione;
- efficacia dell'anonimizzazione/cancellazione: adottare misure efficaci per assicurare la non reidentificazione dei dati anonimizzati o il recupero dei dati cancellati;
- automatizzazione: automatizzare il più possibile la cancellazione dei dati personali non necessari;
- criteri di conservazione: stabilire la durata della conservazione dei dati personali identificandoli rispetto alla specifica finalità;
- giustificazione: capacità di documentare la determinazione del periodo di conservazione rispetto alla finalità individuata;
- applicazione delle politiche di conservazione: adottare politiche di conservazione interne e verificare la loro applicazione;
- registri di eventi: definire i dati personali necessari per i registri di eventi;
- flusso di dati: monitorare il flusso di dati personali e la generazione delle copie, limitandone la conservazione anche temporanea.

3.8 Integrità e riservatezza

Ai dati personali trattati, affinché rimangano integri e riservati, devono essere applicate misure tecniche e organizzative adeguate a garantire la protezione da trattamenti illeciti o non autorizzati

nonché da incidenti di violazione dei dati (*data breach*). Sul Titolare grava l'obbligo di valutare costantemente i mezzi del trattamento e le misure di sicurezza scelte attraverso revisioni periodiche delle stesse nonché di dotarsi di una procedura per la gestione delle violazioni dei dati.

Gli elementi da valutare ai fini del principio di integrità e riservatezza dei dati nell'applicazione della *privacy by design e by default* sono:

- sistema di gestione della sicurezza delle informazioni: predisporre strumenti operativi, politiche e procedure per assicurare la sicurezza delle informazioni;
- analisi/valutazione del rischio: valutare costantemente i rischi per la sicurezza dei dati personali e del trattamento, considerando l'impatto sui diritti delle persone, e predisporre misure di contrasto per i rischi identificati;
- standardizzazione delle minacce: definire, attraverso l'analisi riferita alla superficie di attacco di specifici sistemi, una standardizzazione esaustiva, sistematica e realistica delle minacce possibili al fine di ridurre i vettori di attacco e le opportunità di sfruttamento delle vulnerabilità;
- sicurezza fin dalla progettazione: progettare e sviluppare i sistemi tenendo conto dei requisiti di sicurezza appropriati al quadro tecnologico del momento; svolgere costantemente test pertinenti;
- manutenzione: verificare periodicamente software e hardware, sistemi e servizi, prodotti e applicazioni al fine di monitorarne costantemente le vulnerabilità e adottare le relative misure di mitigazione delle stesse;
- gestione del controllo degli accessi: l'accesso ai dati deve essere limitato al solo personale autorizzato differenziando i privilegi di accesso secondo i seguenti criteri:
- limitazione dell'accesso: progettare il trattamento dei dati in modo tale che accedano ai dati un numero minimo di persone;
- limitazione al contenuto dei dati: differenziare e limitare l'accesso ai dati sia rispetto allo svolgimento della singola operazione, sia agli ambiti di competenza del rispettivo dipendente autorizzato al trattamento;
- segregazione dell'accesso: progettare il trattamento in modo da evitare l'accesso totale ai dati degli interessati o di categorie specifiche degli stessi;
- trasferimenti sicuri: proteggere la trasmissione di dati da modifiche e accessi non autorizzati e/o accidentali;
- conservazione sicura: proteggere la conservazione dei dati da modifiche e accessi non autorizzati attraverso procedure per valutare il rischio di conservazione centralizzata o decentrata sulle categorie di dati personali a cui si applicano adottando all'occorrenza misure di sicurezza adeguate. In caso di rischio elevato il Titolare è tenuto ad adottare sistemi di cifratura dei dati personali;
- pseudonimizzazione e cifratura: pseudonimizzare i dati personali e cifrare i backup/registri di eventi come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni;
- backup/registri di eventi: conservare backup e registri di eventi nella misura necessaria per la sicurezza delle informazioni e utilizzarli su base routinaria al fine di monitorare gli eventi e adempiere ai controlli di sicurezza prevedendo revisioni periodiche;
- ripristino in caso di disastro (*disaster recovery*/continuità operativa): prevedere procedure di ripristino del sistema informativo in caso di disastro al fine di garantire la continuità operativa (*business continuity*) e di ripristinare velocemente la disponibilità dei dati personali in caso di incidenti rilevanti;
- protezione in base al rischio: proteggere le categorie di dati personali contro il rischio di violazioni della sicurezza con misure di sicurezza adeguate; tenere separati i dati che comportano rischi particolari dagli altri dati personali, adottando misure più elevate quali la cifratura;

- gestione della risposta in caso di incidenti legati alla sicurezza: predisporre metodologie e procedure finalizzate a rilevare, limitare, gestire e segnalare le violazioni dei dati e prevedere dei processi di *lesson learned*;
- gestione delle violazioni di dati personali: disporre procedure di gestione degli incidenti di sicurezza e delle violazioni di dati personali, comprese procedure di notifica quali la gestione delle notifiche verso l'Autorità e di comunicazione verso gli interessati.

3.9 Responsabilizzazione

Ai fini dell'applicazione del principio di responsabilizzazione il Titolare deve conoscere ed attuare le norme europee e nazionali in materia di protezione dei dati adempiendo ai relativi obblighi. Il Titolare è responsabile che le attività di trattamento siano conformi a tutti i principi enunciati ai punti che precedono e deve essere in grado di dimostrare e documentare tale conformità, comprovando gli effetti delle misure adottate per tutelare i diritti degli interessati e i motivi per cui tali misure sono considerate adeguate ed efficaci.

4. UTILIZZO DELLE CERTIFICAZIONI (art. 25, paragrafo 3 RGPD)

Ai sensi dell'articolo 25, par. 3 del RGPD il Titolare del trattamento può utilizzare le certificazioni di cui all'articolo 42 RGPD come un elemento per dimostrare la conformità dei trattamenti ai principi di *privacy by design e by default*.

La certificazione di un trattamento svolto da parte di un Titolare o di un Responsabile, ai sensi dell'articolo 42 del RGPD, costituisce, all'occorrenza, un elemento di valutazione della conformità dello stesso con il RGPD, con particolare riferimento ai principi di *privacy by design e by default,* anche da parte dell'Autorità.

Qualora il Titolare voglia avviare una procedura di certificazione può utilizzare, ai fini del conseguimento della stessa, la documentazione *privacy* che dimostra l'applicazione dei principi di *privacy by design e by default* ai trattamenti di competenza.

Anche qualora un trattamento sia certificato ai sensi dell'articolo 42, il Titolare è comunque tenuto a garantire il monitoraggio costante e il miglioramento della conformità ai criteri della *privacy by design e by default* di cui all'articolo 25.

5. *PRIVACY BY DESIGN E BY DEFAULT* NEI TRATTAMENTI BASATI SU SISTEMI DI INTELLIGENZA ARTIFICIALE.

Il Titolare, in coerenza con la normativa europea in tema di intelligenza artificiale[6], è tenuto all'applicazione della presente *policy* anche qualora provveda ad automatizzare le proprie attività ricorrendo a sistemi che utilizzano tecnologie di Intelligenza Artificiale, nella misura in cui comportino il trattamento di dati personali; sia per i trattamenti eseguiti dal Titolare stesso che per quelli eseguiti da un Responsabile del trattamento per suo conto.

---

[6] Il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 (AI Act), entrato in vigore il 1° agosto 2024, all'art. 3, n. 1), definisce un «sistema di IA» quale *"un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"*. L'AI Act inoltre fa espressamente salve le discipline di protezione dei dati personali (cfr. Considerando n. 10 e art. 2, par. 7).

Pertanto, tutte le volte in cui un processo algoritmico di Intelligenza Artificiale coinvolga dati personali il Titolare del trattamento ha l'obbligo di conformarsi e di essere in grado di comprovare il rispetto dei principi e degli adempimenti previsti dal RGPD nonché di aver effettivamente tutelato il diritto alla protezione dei dati personali degli interessati fin dalla progettazione *(privacy by design)* e per impostazione predefinita *(privacy by default)* (artt. 5, 24 e 25, par. 1, del RGPD).

Tenuto conto dell'art. 22 del RGPD che sancisce il generale diritto dell'interessato a non essere soggetto ad una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, quando ciò può produrre effetti giuridici che lo riguardano o incidere in modo significativo sulla sua persona, l'applicazione dei principi di *privacy by design e by default* nei trattamenti di dati personali basati sull'utilizzo di sistemi di Intelligenza Artificiale determina in capo al Titolare del trattamento i seguenti obblighi:

- verificare che il trattamento, in un contesto di interesse pubblico quale quello che
- contraddistingue la Regione, sia specificamente previsto da una base giuridica nel diritto nazionale che assicuri il rispetto dei diritti e delle libertà degli interessati;
- informare gli interessati che il trattamento dei dati personali avviene attraverso algoritmi, fornendo informazioni significative sulla logica utilizzata, sì da poterla comprendere (principio di conoscibilità);
- assicurare sempre la possibilità di un intervento umano al fine di garantire l'individuazione di eventuali distorsioni dei processi automatizzati e di assicurare all'interessato di poter esprimere la propria opinione, nonché di contestare eventuali decisioni generate dal sistema (principio di non esclusività della decisione algoritmica);
- verificare l'imparzialità degli algoritmi utilizzati in modo che gli stessi siano conformi alle finalità del trattamento e imparziali rispetto alle stesse (principio di non discriminazione algoritmica);
- effettuare una attenta valutazione di impatto (DPIA) sui diritti e le libertà degli interessati ai sensi degli artt. 35-36 del RGPD;
- adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita;
- verificare costantemente che le misure adottate ai fini della tutela dei diritti e delle libertà dell'interessato siano adeguate ed efficaci anche nel tempo prevedendo periodiche verifiche e revisioni.

6. CONSEGUENZE DELLA NON CONFORMITA' DEL TRATTAMENTO AI PRINCIPI DI *PRIVACY BY DESIGN E BY DEFAULT*

Nelle procedure indicate all'articolo 58 RGPD, la non conformità dei trattamenti all'art. 25 RGPD, può costituire per l'Autorità' di controllo elemento di valutazione nell'esercizio dei poteri correttivi e sanzionatori ad essa attribuiti che, ai sensi dell'art. 58, par. 2, RGPD possono comprendere avvertimenti, ammonimenti, ingiunzioni di conformarsi ai diritti degli interessati, limitazioni o divieti di trattamento nonché sanzioni amministrative pecuniarie.

L'applicazione dei principi di *privacy by design e by default*, inoltre, ai sensi dell'art. 83 RGPD, rileva anche come elemento di determinazione, da parte dell'Autorità, dell'ammontare delle sanzioni pecuniarie per le violazioni del RGPD.