Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

AL27

PROCEDURA INTERNA AVENTE AD OGGETTO LA VALUTAZIONE CIRCA L'OBBLIGATORIETA' O L'OPPORTUNITA' DI REDIGERE UNA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE, (P. IVA: 09323530965) (infra "ASST RHODENSE"), in persona del suo legale rappresentante pro tempore, con sede legale in Garbagnate Milanese (MI), viale Forlanini, 95, intende illustrare – in ossequio al combinato disposto tra gli artt. 5 paragrafo 2), 24 paragrafi 1) e 2), 25, 35 e Considerando n. 75), 76), 83), 84), 89) – 95) del Regolamento UE n. 2016/679 (GDPR) – il formale processo volto a valutare, nel rispetto del (fondamentale) principio di accountability (o responsabilizzazione), l'obbligatorietà o comunque l'opportunità di redigere una Valutazione d'Impatto sulla protezione dei dati personali (DPIA) in ossequio all'art. 35 del GDPR.

1. Introduzione.

L'art. 35 paragrafo 1) del GDPR impone al Titolare del trattamento di effettuare, prima di procedere alla relativa attività di trattamento, una DPIA, laddove essa – considerata la natura, l'oggetto, il contesto e le finalità – possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche interessate dal trattamento in esame[1].

Nel dettaglio, una DPIA consiste in una procedura finalizzata a descrivere il trattamento, a valutare la sua necessità e la sua proporzionalità, ed a facilitare la gestione dei rischi[2] per i diritti e le libertà delle persone fisiche[3] derivanti dal trattamento dei loro dati personali: in sintesi, la DPIA è un'importante strumento in termini di accountability, giacché aiuta il Titolare non soltanto a rispettare le prescrizioni relative alla normativa comunitaria e nazionale sulla protezione dei dati personali, ma anche a dimostrare l'adozione di misure di sicurezza tecniche ed organizzative idonee a garantire il rispetto di tali precetti.

A tal riguardo, si aggiunge, infine, che l'eventuale inosservanza degli oneri relativi alla DPIA (es. mancato svolgimento o esecuzione non corretta; mancata consultazione preventiva al Garante Privacy ex art. 36 del GDPR) può comportare l'applicazione della sanzione amministrativa di cui all'art. 83 paragrafo 4) lettera a) del GDPR.

2. Operazioni di trattamento soggette alla DPIA.

Come anticipato, il GDPR non impone di condurre una DPIA con riguardo ad ogni trattamento che possa comportare rischi per i diritti e le libertà delle persone fisiche, bensì **essa è obbligatoria solo qualora un trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche**", così come chiarito dall'art. 35 paragrafi 1), 3) e 4) del GDPR; tuttavia, si precisa che, laddove la necessità di una DPIA non emerga con chiarezza, il WP 29 raccomanda di farvi comunque ricorso, dato che essa contribuisce all'osservanza, da parte del Titolare, delle norme in materia di data protection.

Tanto premesso, ai sensi dell'art. 35 paragrafo 4) del GDPR, il Garante Privacy ha provveduto, all'interno dell'Allegato 1) del Provvedimento del 11.10.2018, a pubblicare un elenco, tuttavia non esaustivo, di tipologie di trattamento soggette al requisito della DPIA[4], tenuto, peraltro, conto dei nove (macro) criteri espressi, sul punto, dal WP 29 nelle Linee Guida n. 248/2017[5]:

---

[1] E' bene precisare che l'art. 35 paragrafo 11) del GDPR ammette espressamente la possibilità che il Titolare effettui nuovamente la DPIA "se necessario", ossia in tutti quei casi in cui "sorgono variazioni del rischio rappresentato dalle attività relative al trattamento". Dunque, pur mancando l'elemento della regolarità (tipico della valutazione del livello di sicurezza), anche la DPIA richiede un preesame di tutti i trattamenti censiti nel Registro ex art. 30 del GDPR, con riferimento al loro livello di rischio per i diritti e le libertà per le persone fisiche, ed un riesame al modificarsi dei rischi, al fine di garantire che sia data concreta applicazione alla protezione dei dati personali.

[2] Per "rischio" deve intendersi lo scenario descrittivo di un evento e delle relative conseguenze, stimate in termini di gravità e di probabilità.

[3] Come chiarito dal WP 29, il riferimento ai "diritti e le libertà" degli interessati va inteso, in primo luogo, come relativo al diritto alla protezione dei dati personali, ma può riguardare anche altri diritti fondamentali, quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

[4] Esempi di casistiche ove, a parere del WP 29, è necessario redigere la DPIA: struttura sanitaria che tratta dati genetici e sanitari di un paziente; controllo sistematico dell'attività dei

I. 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";
II. 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 essere parte di un contratto in essere;
III. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso una rete, effettuati anche online o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione;
IV. Trattamenti su larga scala di dati aventi carattere estremamente personale[6];
V. 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;
VI. Trattamenti (non occasionali) di dati relativi a soggetti vulnerabili (es. minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
VII. 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 online attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità);
VIII. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;

---

lavoratori; istituzione di un database nazionale di valutazione creditizie o per finalità di anti frode; conservazione per scopi di archiviazione di dati cd. sensibili pseudonimizzati relativi a soggetti interessati vulnerabili coinvolti in progetti di ricerca o studi clinici sperimentali.

[5] I nove criteri individuati dal WP 29 sono: i) 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" (es. istituto finanziario che effettua uno 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; una società operante nel settore delle biotecnologie che offre dei test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una società che crea profili comportamentali o di marketing, a partire dalle operazioni o dalla navigazione compiuta sul proprio sito internet); ii) decisioni automatizzate che producono significativi effettivi giuridici o di analoga natura; iii) monitoraggio sistematico; iv) dati sensibili o dati di natura estremamente personale (es. ospedale che conserva le cartelle cliniche dei pazienti; investigatore privato che conserva le informazioni sui soggetti responsabili di reati); v) trattamenti di dati su larga scala (al riguardo, il WP 29 ha individuato una serie di fattori, utili ai fini ermeneutici: 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); vi) combinazione o raffronto di un insieme 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; vii) dati relativi a interessati vulnerabili (in merito, il WP 29 ha precisato che in tale categoria sono, senz'altro, ricompresi i seguenti soggetti: minori; dipendenti; segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (es. soggetti con patologie psichiatriche; richiedenti asilo; anziani; pazienti); ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo Titolare del trattamento); viii) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative; ix) tutti quei trattamenti che, di per sé, "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto" (cfr. art. 22 e Considerando n. 91) del GDPR). A tal riguardo, il WP 29 ha aggiunto, infine, che un Titolare del trattamento può ritenere, in via generale, necessario condurre una DPIA laddove un trattamento soddisfa anche uno solo dei citati criteri.

[6] Es. dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche) 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).

IX. 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);
X. Trattamenti di dati personali cd. particolari ex art. 9 paragrafo 1) del GDPR ovvero di dati personali cd. giudiziari ex art. 10 del GDPR;
XI. Trattamenti sistematici di dati biometrici;
XII. Trattamenti sistematici di dati genetici.

A tal riguardo, occorre, tuttavia, rilevare che sia i criteri (generali) indicati dal WP 29 sia gli scenari individuati, ai sensi dell'art. 35 paragrafo 4) del GDPR, dal Garante Privacy italiano possono naturalmente essere integrati, estesi o, perfino, motivatamente smentiti e disapplicati, a valle di una compiuta analisi dei rischi ed in ossequio al principio di responsabilizzazione; l'individuazione delle casistiche di trattamenti rischiosi, da parte del Titolare del trattamento, deve, comunque, sempre tenere conto, sia nella fase preliminare alla DPIA sia nell'attività di approfondimento svolta nel corso di una valutazione d'impatto, del rischio patologico nonché del rischio fisiologico comportato da quella specifica attività di trattamento di dati personali.
In proposito, il WP 29 ha raccomandato di procedere con la redazione della DPIA, nel caso in cui la sua necessità non emerga con chiarezza.

Orbene, per decidere se effettuare (o meno) una DPIA, è essenziale aver valutato natura, oggetto, contesto e finalità del trattamento, ed aver determinato che effettivamente il trattamento in analisi può presentare un rischio elevato per i diritti e le libertà delle persone fisiche; è, quindi, possibile derivare un criterio (generale) di scelta rispetto alle situazioni in cui è necessario effettuare una DPIA, e cioè che essa deve essere realizzata per tutti quei trattamenti in cui i rischi indicati nel Considerando n. 75) del GDPR, in re ipsa idonei a soddisfare il requisito della "gravità", risultino essere anche "probabili", a seguito della "valutazione oggettiva" di cui al Considerando n. 76) del GDPR.

3. Contenuto della DPIA.
L'art. 35 paragrafo 7) del GDPR (da leggersi, in combinato disposto, con il Considerando n. 84)[7] e 90)[8] del GDPR) ha provveduto ad individuare il contenuto minimo della DPIA, la quale, dunque, si sostanzia nella presenza dei seguenti elementi costitutivi: a) descrizione sistematica dei trattamenti previsti e delle finalità di trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento; b) valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) valutazione dei rischi per i diritti e le libertà degli interessati[9]; d) misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR (ed al Codice Privacy), tenuto conto dei diritti e degli interessi legittimi di soggetti interessati ed eventualmente di altre persone.

[7] Considerando n. 84) del GDPR: "Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo".
[8] Considerando n. 90) del GDPR: "In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento".
[9] Con riferimento alla valutazione dei rischi di cui al punto c), giova sottolineare come non si possa sposare un approccio meramente ingegneristico, tipico delle analisi dei rischi sulla sicurezza informatica, ma, invero, è necessario integrare tale tipologia di analisi tecnica con una più "umanistica" mappatura delle possibili conseguenze negative del trattamento dei dati sui diritti e sulle libertà fondamentali dell'individuo.

Dunque, la DPIA deve permettere di far comprendere quale sia stata, a monte, la riflessione che ha condotto, a valle, all'esecuzione della valutazione stessa, nel rispetto, come già anticipato, del principio di accountability, il quale non si sostanzia solo nel rispetto dei principi di cui all'art. 5 del GDPR, ma, anche e soprattutto, nella capacità, da parte del Titolare del trattamento, di dimostrare di averli osservati: infatti, il contenuto "minimo" della DPIA è volto proprio a rendere effettiva la verificabilità della responsabilizzazione del Titolare del trattamento.

4. DPIA: unico Titolare, Titolari del trattamento differenti o co-Titolarità del trattamento.

Laddove lo stesso Titolare svolge dei trattamenti simili è sufficiente redigere una singola DPIA ai sensi dell'art. 35 paragrafo 1) del GDPR, giacché è ragionevole aspettarsi che questi, avendo caratteristiche pressoché analoghe, comportino i medesimi "rischi elevati"; tuttavia, il Considerando n. 92)[10] del GDPR estende lo svolgimento di una sola DPIA anche a quei trattamenti aventi la stessa natura, oggetto, finalità e contesto, che vengono effettuati da Titolari del trattamento differenti su piattaforme comuni: la ratio di questo accorpamento di valutazioni è, soprattutto, legato al fattore dell'efficacia e dell'efficienza in termini economici e di tempistiche, in quanto richiedere singole valutazioni per trattamenti pressoché identici, ancorché effettuati da Titolari del trattamento diversi, sarebbe effettivamente inutile.

Infine, nel caso in cui un trattamento venga svolto in regime di co-titolarità ex art. 26 del GDPR, è necessario che ciascun co-Titolare definisca, in modo preciso, gli obblighi rispettivamente incombenti: nello specifico, la DPIA deve stabilire, inter alia, chi possiede la responsabilità delle singole misure finalizzate alla gestione dei rischi ed alla tutela dei diritti e delle libertà degli interessati; inoltre, ciascun co-Titolare deve indicare, con chiarezza, le rispettive esigenze, e condividere tutte le informazioni utili, senza, tuttavia, pregiudicare quanto coperto da segreto (es. informazioni economiche riservate, tutelate dal segreto commerciale o soggette a diritti di proprietà intellettuale) né rivelare eventuali vulnerabilità.

5. Conduzione della DPIA.

Ai sensi dell'art. 35 paragrafo 2) del GDPR, spetta al Titolare del trattamento garantire l'effettuazione della DPIA, la cui conduzione materiale può, tuttavia, essere affidata ad un altro soggetto interno o esterno alla propria organizzazione (pur permanendo, nel caso, la responsabilità (ultima) in capo al relativo Titolare del trattamento); nell'effettuare tale adempimento, il Titolare deve consultarsi con il proprio Responsabile della protezione dei dati, ove designato, il quale ha, peraltro, l'onere di monitorare lo svolgimento della DPIA medesima ai sensi dell'art. 39 paragrafo 1) lettera c) del GDPR.

Se il trattamento è svolto, in tutto o in parte, da un Responsabile, quest'ultimo deve assistere il Titolare nella conduzione della DPIA, fornendo ogni informazione necessaria conformemente all'art. 28 paragrafo 3) lettera f) del GDPR.

Infine, il Titolare del trattamento deve raccogliere, se del caso, le "opinioni degli interessati o dei loro rappresenti" (art. 35 paragrafo 9) del GDPR): a tal proposito, il WP 29 ha precisato quanto segue: i) per la raccolta delle opinioni in questione si possono individuare molteplici modalità, in rapporto al contesto (es. uno studio generico relativo a finalità e mezzi del trattamento; un quesito rivolto ai rappresentanti del personale; un questionario inviato ai futuri clienti del Titolare del trattamento); ii) qualora la decisione assunta, in ultima analisi, dal Titolare si discosti dall'opinione dei soggetti interessati, è bene che il Titolare documenti le motivazioni che hanno condotto alla prosecuzione o meno del progetto; iii) il Titolare dovrebbe documentare anche le motivazioni della mancata consultazione degli interessati, qualora decida che quest'ultima non sia opportuna (es. in quanto potrebbe pregiudicare la riservatezza dei piani aziendali, oppure poiché sproporzionata o impraticabile).

6. Revisione di una DPIA.

[10] Considerando n. 92) del GDPR: "Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata".

Dato che le attività di trattamento tendono, in via generale, ad evolvere rapidamente e, pertanto, presentano nuove vulnerabilità, si osserva come pare opportuno (se non doveroso) sottoporre la DPIA ad una revisione ad intervalli regolari, ai fini di un miglioramento continuo nonché per mantenere (inalterato) il livello di protezione dei dati al mutare del tempo; infatti, come correttamente sottolineato dal WP 29, lo svolgimento della DPIA rappresenta, invero, un processo continuativo (e non un'attività una tantum).

7. Consultazione del Garante Privacy.

Come già anticipato, la DPIA è necessaria laddove un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, riguardo al quale è onere del Titolare del trattamento individuare le misure di sicurezza (tecniche ed organizzative) volte a ridurre tale rischio ad un livello accettabile (e dimostrare l'osservanza del GDPR e del Codice Privacy).

Tuttavia, nel caso in cui il Titolare del trattamento non sia in grado di individuare misure sufficienti a ridurre il rischio a livelli accettabili (ossia, qualora il rischio residuale continui a permanere elevato), è necessario consultare il Garante Privacy ai sensi dell'art. 36 del GDPR.

8. Il valore della DPIA: espressione dei principi di privacy by design e di privacy by default.

A conclusione del quadro delineato sull'effettuazione della DPIA (e sui suoi possibili risvolti), è possibile, infine, evidenziarne il legame con i principi di data protection by design e by default: infatti, la DPIA rappresenta uno strumento utile per il Titolare del trattamento non soltanto al fine di rispettare il principio di responsabilizzazione di cui all'art. 5 paragrafo 2) del GDPR, ma anche per affrontare gli aspetti di protezione dei dati prima che il prodotto o il servizio vengano messi sul mercato.

Garbagnate Milanese (MI), lì 9.11.2022 (data di ultimo aggiornamento).

AZIENDA SOCIO-SANITARIA TERRITORIALE RHODENSE
(in persona del suo legale rappresentante pro tempore)