Ordine delle Professioni Infermieristiche di Ferrara

Procedura per la Valutazione di Impatto sulla Protezione dei Dati [1]

L'**Ordine delle Professioni Infermieristiche di Ferrara** (C.F.: 80006200382), corrente in Ferrara, via del Naviglio 33/A, in qualità di Titolare del trattamento ed alla luce di quanto previsto dalla disciplina europea e nazionale in materia di protezione di dati personali[2], ha approvato nella riunione del Consiglio Direttivo del 19/05/2022 – previo parere del Responsabile per la Protezione dei Dati designato – la seguente procedura, disponendo che sia distribuita ai dipendenti ed agli stessi venga erogata l'opportuna attività di formazione.

*****

INDICE

[1] La presente procedura viene predisposta anche ai sensi e per gli effetti degli artt. 35 e seguenti del Regolamento del Parlamento europeo e del Consiglio del 27/4/2016, n. 679, relativi alla notifica all'Autorità di Controllo ed alla comunicazione agli interessati di eventuali violazioni dei dati personali.

[2] Regolamento del Parlamento europeo e del Consiglio del 27/4/2016, n. 679 (d'ora in avanti, per brevità, "*GDPR*") e Decreto Legislativo 30/6/2003, n. 196 s.m.i. (anche con riferimento a quanto previsto dal Decreto Legislativo 10/8/2018, n. 101) (nel prosieguo, più brevemente, "*Codice Privacy*").

1. Campo di applicazione

Secondo quanto prescritto dalla disciplina in materia di protezione dei dati personali applicabile, i Titolari sono tenuti a valutare i rischi legati ai processi e attività aziendali quando un tipo di trattamento preveda, in particolare, l'uso di nuove tecnologie e, considerando la sua natura, il suo oggetto, il contesto e le sue finalità, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Lo scopo di tale Valutazione di Impatto sulla Protezione dei Dati (Data Protection Impact Assessment, "*DPIA"*) è quello di aumentare la consapevolezza del rischio e mettere in atto le opportune misure per prevenire il verificarsi di eventi che possano produrre un impatto negativo sui dati.
La presente procedura definisce in che modo rispettare l'obbligo di legge appena descritto, ha decorrenza immediata è destinata a tutti i dipendenti dell'Ordine.

2. Definizioni rilevanti

Ai fini della presente procedura:

- per "***dato personale***" si intende 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.

- per "***dati appartenenti a particolari categorie***" si intendono: i dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare la vita sessuale, i dati giudiziari, i dati relativi alla salute, i dati genetici e i dati biometrici.

- per "***trattamento***" si intende 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.

- per "***profilazione***" si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

- per "***processo decisionale automatizzato***" si intende un processo organizzativo che sia governato da uno strumento che consente di prendere decisioni impiegando mezzi tecnologici (ad esempio, un algoritmo) con o senza l'intervento di un soggetto che sia in grado di influenzarne o modificarne l'esito (ad esempio, il sito di un'assicurazione online che proponga in automatico un premio della polizza RCA sulla base del reddito dell'assicurato).

3. *Riferimenti normativi*

- GDPR – Regolamento del Parlamento europeo e del Consiglio del 27/4/2016, n. 679
- CODICE PRIVACY – Decreto Legislativo 30 giugno 2003, n. 196 s.m.i.
- DECRETO ATTUATIVO – Decreto Legislativo 10 agosto 2018, n. 101
- Provvedimento dell'11 ottobre 2018, n. 467 del Garante per la Protezione dei Dati Personali "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione di impatto sulla protezione dei dati*"
- 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 – Gruppo di Lavoro Articolo 29 per la Protezione dei Dati – Ottobre 2017
- Handbook on Security of Personal Data Processing – ENISA European Union Agency for Cybersecurity – Gennaio 2018

4. *Ruoli e responsabilità*

UFFICIO/RUOLO	RESPONSABILITÀ
Consiglio Direttivo	Ha la responsabilità di assicurare l'applicazione della presente procedura per valutare l'impatto del nuovo trattamento – o delle significative modifiche progettate ad un trattamento già in corso – al fine di comprendere i rischi incidenti sui diritti e le libertà delle persone fisiche cui si riferiscano i dati personali coinvolti.
Responsabile per la Protezione dei Dati	Ha la responsabilità di assistere il Consiglio Direttivo, fornendo consulenza e supporto, se richiesti, durante la Valutazione di Impatto sulla Protezione dei Dati.
Titolare del trattamento (legalmente rappresentato dal Presidente del Consiglio Direttivo)	Ha la responsabilità di promuovere la tempestiva applicazione della procedura, vigilando affinché sia conclusa prima dell'inizio del nuovo trattamento, valutando le caratteristiche del nuovo Progetto e decidendo in ordine alla necessità di accedere alla Consultazione Preventiva nei casi previsti dalla legge[3].

5. *Metodologia*

I nuovi trattamenti che rientrano nelle seguenti categorie dovranno essere soggetti a DPIA:

- ***trattamenti di dati appartenenti a particolari categorie***
- ***trattamenti inclusivi di profilazione, che comportino una valutazione e/o l'assegnazione di un punteggio all'interessato***
- ***trattamenti inclusivi di processi decisionali automatizzati, che abbiano effetto giuridico o incidano in modo analogamente significativo sull'interessato***
- ***trattamenti di dati personali svolti su larga scala***
  Il concetto di "*larga scala*" è da intendersi riferito al numero di soggetti interessati (in termini assoluti, ovvero espressi in percentuale della popolazione di riferimento), al volume

[3] Ai sensi e per gli effetti dell'art. 36 GDPR.

ed alla tipologia di dati trattati, alla durata o persistenza, nonché alla portata geografica delle attività di trattamento, raffrontato ad attività svolte da Titolari di trattamento analoghi per dimensioni, operanti nel medesimo contesto, di mercato e territoriale.

- ***combinazione o raffronto di insiemi di dati personali***
  ad esempio, derivanti da due o più trattamenti svolti per finalità differenti o da Titolari distinti.
- ***dati personali relativi ad interessati vulnerabili***
  ad esempio, i minori e ogni interessato per il quale possa identificarsi una situazione di squilibrio con il Titolare.
- ***utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative***
  ad esempio, applicazioni mobile, legate ad Internet o ad alta innovazione

Devono inoltre essere oggetto di preventiva DPIA le tipologie di trattamento che rientrano nell'elenco redatto dall'Autorità di Controllo (incluso, per l'Italia, nel Provvedimento dell'11 ottobre 2018, n. 467 del Garante per la Protezione dei Dati Personali "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione di impatto sulla protezione dei dati*", disponibile sul sito istituzionale).

La DPIA è un processo qualitativo ed un elevato numero di fattori deve essere preso in considerazione dal Titolare, come, ad esempio, i tipi di dati personali, la criticità dell'operazione di elaborazione, il volume dei dati personali, le categorie speciali di soggetti e il danno derivante dalla perdita di riservatezza, integrità e disponibilità dei dati.
L'approccio scelto si basa su di un processo di valutazione del rischio, articolato in quattro fasi:

- definizione dell'attività di elaborazione e del suo contesto;
- comprensione e valutazione dell'impatto;
- definizione di possibili minacce e valutazione della probabilità che queste si verifichino;
- valutazione del rischio (combinando la probabilità e l'impatto/danno dell'evento in questione).

Ad esito di tale processo, il Consiglio Direttivo adotta misure di sicurezza tecniche e organizzative appropriate al livello di rischio.

Saranno considerati, in quest'ottica, cinque livelli di impatto, articolati come segue (**tabella 1**):

gravità/danno	**definizioni/criteri**
4 massimo	Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che compromettono severamente i loro diritti e libertà
3 importante	Gli interessati potrebbero avere conseguenze significative sui loro diritti e libertà, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative
2 limitato	Gli interessati potrebbero sperimentare inconvenienti significativi sui loro diritti e libertà, che saranno in grado di superare nonostante alcune difficoltà
1 trascurabile	Gli interessati non subiranno alcun impatto sui loro diritti e libertà o potrebbero incontrare qualche inconveniente, che supereranno senza difficoltà
0 indefinito	L'impatto per gli interessati è talmente lieve da non essere stimabile

Il livello di probabilità che si possa verificare una minaccia può essere definito, per ciascuna delle aree di valutazione, come segue (**tabella 2**):

gravità/danno	definizioni/criteri
4 massima	Basandosi sugli asset organizzativi, sembra estremamente facile che le fonti di rischio considerate possano creare una minaccia (ad esempio, il furto di supporti cartacei conservati nella sala pubblica dell'Ordine).
3 importante	Basandosi sugli asset organizzativi, sembra possibile che le fonti di rischio considerate possano creare una minaccia (ad esempio, il furto di supporti cartacei conservati negli uffici dell'Ordine il cui accesso è controllato da una persona all'ingresso).
2 limitata	Basandosi sugli asset organizzativi, sembra difficile che le fonti di rischio considerate possano creare una minaccia (ad esempio, il furto di supporti cartacei conservati in un locale dell'Ordine il cui accesso è controllato mediante chiave, adeguatamente custodita).
1 trascurabile	Basandosi sugli asset organizzativi, non sembra possibile che le fonti di rischio considerate possano creare una minaccia (ad esempio, il furto di supporti cartacei conservati in un locale dell'Ordine il cui accesso è controllato mediante chiave, adeguatamente custodita, ed allarme perimetrale).
0 indefinita/improbabile	Non c'è una reale possibilità che il rischio si concretizzi.

Dopo aver valutato l'impatto del concretizzarsi di rischi su operazioni di trattamento dei dati e la relativa probabilità che si verifichi una minaccia, è possibile effettuare una valutazione finale del rischio secondo la formula:

$$R = P \times D$$

che associa i due parametri che determinano il rischio stesso, cioè la probabilità di accadimento e la gravità delle possibili conseguenze.

6. Procedura

Per applicare la presente procedura l'Ordine si è dotato di uno strumento per l'implementazione della presente procedura, al fine di guidare i Reparti aziendali coinvolti nell'esecuzione, controllo e validazione secondo un approccio strutturato e guidato.

Lo strumento di riferimento scelto si basa sul software (*PIA* versione 3.0.3 – maggiori informazioni disponibili al sito) messo a disposizione dal CNIL (*Commission National Informatique & Libertés*), Autorità di Controllo francese, per i Titolari del trattamento, che garantisce:

- un'interfaccia didattica allo svolgimento della procedura che guida l'utente, secondo dei parametri definiti e validati da enti di garanzia e controllo europei (per poter visualizzare alcune indicazioni di utilizzo si consiglia di seguire il video tutorial);
- una presentazione degli aspetti legali e tecnici in grado di costituire un repository di informazioni facilmente fruibili e utilizzabili da tutte le parti coinvolte;
- modularità di approccio;
- una modalità di controllo, revisione e approvazione strutturata.

7. Controlli e sanzioni

La presente procedura entra in vigore a partire dalla data di approvazione da parte del Consiglio Direttivo e le sua mancata osservanza comporta il rischio di un intervento disciplinare, in linea con quanto previsto dallo Statuto dei Lavoratori e dal Contratto Collettivo Nazionale di Lavoro applicabile.

*****

Ferrara, 19/05/2022

Il Segretario
Valentina Michelini

Il Presidente
Simone Vincenzi