RAPPORTO ANNUALE DEL DPO

REGOLAMENTO UE 679/2016

18 GENNAIO 2024

ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DELLA PROVINCIA DI TERAMO
VIA BRIGIOTTI, 12 – 64100 – TERAMO (TE)

Rapporto Annuale del DPO sulle attività di trattamento e protezione dei dati dell'Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Teramo

Nome del DPO: LAZZARI MARCO

Soggetti contattati nell'ambito dell'organizzazione:
Presidente Legale Rappresentante
Direttore Amministrativo

Periodo di osservazione dell'attività di audit: 01/01/2023 – 31/12/2023
Data di emissione del rapporto: 18/01/2024

Sommario

1 Premessa

Questa Relazione Annuale è stata sviluppato dal DPO, che il Titolare del Trattamento ha designato con apposita procedura ai sensi dell'art. 37 del Reg. UE 679/2016, nel pieno rispetto dei dettati del regolamento in materia di protezione dei dati personali e successive integrazioni e modificazioni.

La presente relazione tiene conto dell'art. 38, paragrafo 3, che prevede che il Data Protection Officer (DPO) "*riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento".*

2 Obbiettivi del Documento

La presente relazione viene emessa sulla base degli incontri effettuati nell'anno 2023, in cui il sottoscritto si è confrontato con la direzione sulla verifica della documentazione di accountability realizzata e sulle azioni di miglioramento consigliate, nei quali sono emersi alcuni spunti che si vanno di seguito a segnalare nell'ottica di fornire supporto per implementare il livello di compliance al dettato del Regolamento UE 2016/679, dal Codice in materia di protezione dati personali (d.lgs 196/2003 novellato dal D.Lgs 101/2018), dai Provvedimenti e dalle Linee Guida fornite dall'Autorità Garante per la protezione dei dati personali, nonché dal Comitato dei garanti Europei "European Protection Board" (EDPB) e dalle linee Guida AGID.

1. Gestione delle attività svolte nella realizzazione della documentazione relativa alla protezione dei dati

ELENCO DEI DOCUMENTI ESAMINATI			
DOC. NR.	TITOLO	SI/NO	NOTE
001	Organigramma funzionale	SI	
002	Nomine Autorizzati/ Incaricati - Designati	SI	
003	Registro dei Trattamenti	SI	
004	Documento Valutazione dei Rischi	SI	
005	Data protection Impact Assessment	SI	
006	Procedura gestione data breach	SI	
007	Accordi/Contratti	SI	
008	Procedure	SI	
009	Policy Interne	SI	
010	Disciplinare interno internet e p.e.	SI	
011	Rapporti Con Interessati: Informativa	SI	
012	CERTIFICAZIONI	SI	
013	CODICI DI CONDOTTA	N.A.	

La attività di audit hanno evidenziato fino a che punto sono attuati i principi di responsabilità nella protezione dei dati, le politiche e le procedure, i controlli in grado di misurare il livello di prestazione della protezione, i meccanismi di individuazione e segnalazione della congruità con i vigenti regolamenti in materia di protezione dei dati personali;

3 Sintesi delle risultanze delle attività

1. Aree esaminate

1. Gestione della protezione dei dati;
2. Addestramento e sensibilizzazione;
3. Gestione manuale ed elettronica dei dati personali;
4. Sicurezza dei dati personali;
5. Congruità dell'informativa;
6. Correttezza delle procedure di raccolta del consenso;
7. Determinazione del tempo di conservazione del dato;
8. Attività di comunicazione e diffusione di dati personali;
9. Attività di trattamento svolte in ambito web e Social Network
10. Violazioni e data breach
11. Esercizio dei diritti degli interessati
12. Registro dei trattamenti
13. Linee Guida AGID
14. Segnalazione Illeciti amministrativi
15. sito internet

Nel contesto dei predetti incontri sono stati affrontati i seguenti argomenti ed effettuate le seguenti attività di controllo:

- Effettuazione delle attività indicate dal sottoscritto, come da ex art. 39 lett. a) GDPR, nel contesto della relazione annuale precedente;
- Verifica del Modello Organizzativo Privacy e allegati;
- Verifica del **Registro dei trattamenti** con indicazioni per il suo aggiornamento/completamento;
- analisi dell'**organigramma** e dell'assetto organizzativo del titolare del trattamento;
- analisi, aggiornamento e revisione delle **informative e dei moduli di acquisizione del consenso** (laddove necessario quale base giuridica del trattamento eseguito);
- Verifica a campione dell'applicazione delle procedure di trattamento da parte degli autorizzati;
- controllo, revisione e aggiornamento delle policy presenti sui **siti web del titolare**;
- controllo del sistema di gestione per l'eventuale realizzazione della **valutazione di impatto**: (tenuto conto degli artt. 32 e 35 del Reg. Ue 16/679 e del Provvedimento del Garante Privacy "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" *(Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018);*
- verifica del livello di attenzione relativamente ai **rischi connessi all'utilizzo di sistemi informatici** e disamina dell'applicazione delle linee Guida AGID;
- Monitoraggio su Linee Guida AGID;
- verifica delle procedure di gestione dell'eventuale violazione di sicurezza ("**data breach**") e dell'eventuale **esercizio di un diritto o di un reclamo** da parte degli interessati;
- Verifica dei rapporti con Fornitori in qualità di Responsabili del Trattamento ai sensi dell'art. 28
- Monitoraggio Recepimento D.Lgs 24/02023 Whistleblowing

CONTROLLO ADEMPIMENTI EFFETTUATI			
ID	**INFORMATIVE**	EFFETTUATO SI/NO	NOTE
001	Informative clienti, dipendenti ecc.	SI	
002	Consenso	SI	Ove necessario per attività accessorie
ID	**ADEGUAMENTO INFORMATICO**		
003	Sistema Operativo	SI	
004	Antivirus	SI	
005	Firewall	SI	
006	Crittografia Hard Disk	SI	

007	Backup	SI	
008	Supporto Backup	SI	
009	Password personalizzate	SI	
010	Account Profili di Autorizzazione	SI	
011	Rete interna protetta	SI	
012	WiFi Guest Visitatori	SI	
ID	**ADEGUAMENTO SITO INTERNET**		
013	Informativa Contatti	SI	
014	Policy Privacy	SI	
015	Cookie Low	SI	
016	Informativa Newsletter	N.A.	
017	Protezione Navigazione SSL	SI	
018	Pagina Social	N.A.	
ID	**ASSETTO ORGANIZZATIVO**		
019	Lettere di Incarico autorizzati interni	SI	secondo le indicazioni del primo comma dell'art. 2 *quaterdecies* del codice privacy
020	Individuazione e Atto di nomina Resp. Esterni	SI	
021	Amministratore di Sistema	SI	
ID	**FORMAZIONE**		
022	Istruzioni all'incaricato	SI	
023	Formazione autorizzati	SI	
024	policy operative	SI	
025	Procedure Operative	SI	
ID	**SICUREZZA TRATTAMENTO DATI**		
026	Registro dei Trattamenti		Il RPD conduce con cadenza semestrale il monitoraggio del Registro delle attività di trattamento, che costituisce uno dei principali elementi di accountability del Titolare dei trattamenti, in quanto fornisce un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione ed è indispensabile per ogni attività di valutazione o analisi del rischio di violazione dei diritti delle persone
027	Determinazione della Durata del trattamento	SI	
028	Classificazione del rischio sui trattamenti	SI	
029	Valutazione di Impatto	SI	La valutazione di impatto sulla protezione dei dati (DPIA) è un processo finalizzato – di norma a seguito di modifiche tecnologiche od organizzative - a riesaminare il trattamento dei dati, valutarne la necessità e la proporzionalità in termini di minimizzazione dei dati utilizzati e dei tempi di conservazione, esaminarne i rischi per i diritti e le libertà delle persone fisiche destinatarie del trattamento e determinare le misure di sicurezza per mitigarli.
030	Valutazione dei rischi	SI	L'analisi è condotta di norma nell'ambito di incontri con i Servizi, nei quali vengono approfondite le caratteristiche dei singoli trattamenti nel contesto delle attività svolte per

			verificarne la corrispondenza con le informazioni dichiarate nel Registro dei trattamenti
031	Smart working	SI	
032	Whistleblowing	SI	In applicazione del D.Lgs 24/2023

2. Addestramento e sensibilizzazione

Sono state realizzate attività di formazione, impartita a tutti i soggetti coinvolti nella protezione e trattamento dei dati personali, con temi specifici volti a sensibilizzare la delicatezza della materia, nonchè la dettagliata conoscenza dei requisiti in materia di protezione dei dati personali, in relazione ai ruoli ed alle responsabilità dei singoli soggetti coinvolti
Atteso che solo gli incaricati regolarmente istruiti possono accedere al trattamento dati, sono in progetto ulteriori incontri formativi allo scopo di Formare tutti gli operatori coinvolti.

3. Gestione manuale ed elettronica dei dati personali

Sono state impartite istruzioni specifiche per adeguare tutti gli strumenti elettronici al fine di rispettare le disposizioni del Reg. UE in riferimento alla protezione dei dati, verificando i processi attuati dall'organizzazione per la gestione di supporti, sia manuali (cartacei) sia elettronici, che contengono dati personali. Le istruzioni sono state rivolte altresì al fine di gestire la creazione, la manutenzione, l'archiviazione, il trasporto, la conservazione e la distruzione di supporti contenenti dati personali.

4. Sicurezza dei dati personali

Le attività di audit hanno verificato che le misure tecniche ed organizzative in essere, siano in grado di garantire un adeguato livello di sicurezza dei dati personali, custoditi su supporti cartacei od elettronici. Sono state impartite istruzioni specifiche in merito alle singole attività di trattamento in merito alle giuste procedure da seguire per garantire la sicurezza degli strumenti e delle strutture.
Si ravvisa la necessità di realizzare un inventario degli asset informatici con relativa valutazione dei rischi al fine di individuare le eventuali criticità e adottare le misure di sicurezza.

5. Congruità della informativa Privacy

In fase di audit sono state esaminate tutte le varie informative che vengono fornite dal titolare del trattamento. Sono state predisposte informative specifiche per le diverse attività di trattamento svolte.
Si ricorda che l'informativa deve essere fornita all'interessato prima di effettuare il trattamento, quindi prima della raccolta dei dati. Nel caso di dati personali non raccolti direttamente presso l'interessato l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

6. Gestione Sito Internet

E' stata effettuata una verifica del sito internet con raccomandazioni tecnologiche:

7. Richieste afferenti a dati personali

L'attività di audit ha verificato i processi in essere, in grado di rispondere ad una qualsiasi richiesta afferente a dati personali. Queste richieste possono provenire da individui, che richiedano copie dei loro dati, così come richieste provenienti da soggetti terzi. L'attività di audit ha verificato inoltre che eventuali richieste di modifica e cancellazione vengano tempestivamente esaudite, nei limiti dei regolamenti vigenti.

8. Attività di comunicazione e diffusione di dati personali

Sono stati verificati tutti i possibili rapporti con soggetti esterni e le possibili comunicazioni con essi, al fine di stabilire il ruolo e la liceità dei Trattamenti posti in essere.

9. Rapporti con Responsabili esterni e rappresentanti di responsabili

L'attività di audit ha verificato all'esistenza di Responsabili esterni a cui sono affidati alcuni trattamenti, e realizzati i documenti di delega e Atti di nomina specifici.

10. Violazioni e Data Breach

L'analisi degli eventi configurabili come *data breach* in ottemperanza al GDPR è fondamento della *accountability* del Titolare del trattamento, che ha il dovere di mettere in atto nella propria organizzazione tutte le misure atte a prevenire il rischio di trattamento non conforme dei dati personali e di responsabilità civile derivante dalla lesione della riservatezza che rechi un danno agli interessati

Per quanto riguarda eventuali "data breach", si ricorda l'obbligo di dover notificare eventuali violazioni dei dati personali all'Autorità Garante o ai diretti interessati al ricorrere dei presupposti di cui agli artt. 33 e 34 GDPR. Tutte le violazioni devono essere sempre documentate dal titolare.
Nel corso dell'anno non si sono verificati violazioni di banche dati o data breach.

11. Richieste di esercizio dei diritti da parte di interessati

Nel corso dell'anno non si sono verificate richieste di esercizio dei diritti da parte di interessati

12. Whistleblowing

E' stata monitorata la corretta applicazione del D.Lgs 24/2023 relativo al Whistleblowing con la realizzazione della relativa documentazione a supporto, nonché la corretta messa a disposizione del canale di segnalazione informatico degli illeciti.
E' stato monitorato la realizzazione della DPIA con rilascio del relativo parere.

13. Interventi migliorativi impartiti

RACCOMANDAZIONI ORGANIZZATIVE

RACCOMANDAZIONI TECNOLOGICHE

14 Conclusioni della Relazione

In virtù delle risultanze precedentemente definite e specificate, il lavoro svolto è stato incentrato in fase iniziale, e successivamente nel corso dell'anno, sulla individuazione delle metodologie di attività effettivamente svolte, l'individuazione delle peculiarità inerenti il Trattamento Dati in relazione alle attività svolte e le procedure di trattamento effettuate. Le attività di monitoraggio sono state effettuate con cadenza periodica trimestrale, all'interno delle quali sono stati effettuate attività di controllo e verifica dei processi di trattamenti e la verifica delle procedure di sicurezza tecniche e organizzative adottate.
Quanto emerso ha evidenziato in via primaria la necessità che il titolare del trattamento mantenga la massima attenzione nella tenuta del proprio Registro dei trattamenti. Il Registro dei trattamenti rappresenta infatti uno strumento fondamentale, non soltanto ai fini di eventuali controlli da parte dell'Autorità Garante per dimostrare la propria accountability, ma anche al fine di ottenere un quadro aggiornato dei trattamenti in essere all'interno della propria attività. Tale documento è prodromico all'esercizio di una valutazione e un'analisi dei rischi.
Per quanto concerne la gestione dell'organigramma, alla luce degli approfondimenti eseguiti, si è ritenuto non sussista ad oggi alcun rapporto di contitolarità del trattamento.

15 Attività programmate per l'anno 2024

In virtù delle risultanze precedentemente indicate, si indicano di seguito le attività in programma per l'anno 2024:

1. Realizzazione di corsi di formazione ove necessari per completare il percorso formativo base obbligatorio per tutti gli incaricati al trattamento dati;
2. Sopralluoghi di verifica periodici per monitorare e verificare le attività effettivamente realizzate;
3. Monitoraggio della documentazione realizzata e da realizzare in base in relazione alle raccomandazioni impartite e/o in base a nuove disposizioni legislative;
4. effettuare un controllo sui rapporti in essere verificando la presenza dei documenti di attribuzione dell'incarico e/o della nomina a responsabile del trattamento;
5. effettuare un controllo sulla coerente mappatura delle banche dati;
6. Supporto negli adempimenti tecnologici e organizzativi ancora da realizzare;
7. Monitoraggio sulle normative nazionali ed europee di interesse dell'Ente;

Il sottoscritto si rende disponibile per ogni necessario chiarimento.

DATA:	18/01/2024
FIRMA DPO	