AZIENDA OSPEDALIERA SANTA MARIA TERNI

Mod. 10 - Rev. 0.1 – Deliberazione del Commissario Straordinario n° 692 del 06 11 2019

MODELLO DI PROCEDURA PER IL DATA BREACH – (VIOLAZIONI DI DATI)

A. AMBITO

Questa procedura si applica a tutti coloro che, a qualsiasi titolo e posizione, effettuano trattamenti di dati personali per conto dell'Azienda Ospedaliera "S. Maria" di Terni, (di seguito AO Terni).

B. SCOPO

Questa procedura ha lo scopo di permettere ad AO Terni, nella sua qualità di titolare del trattamento, di ottemperare alle prescrizioni contenute negli artt. 33 e 34 del Regolamento Europeo 679/2016 in materia di violazione dei dati personali.

C. RIFERIMENTI

- Artt. 33 e 34 Reg. EU 679/2016 - GDPR.
- WP250 - Guidelines on Personal data breach notification under Regulation 2016/679.
- ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches.

D. DEFINIZIONI

AUTORITA' DI CONTROLLO: si intende l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51. Per l'Italia il Garante per la Protezione dei Dati Personali (GPDP).

COMUNICAZIONE: si intende la comunicazione che deve essere fatta agli interessati a norma dell'art 34, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

INCIDENTE: si intende l'accadimento di un evento non desiderato che comporta la violazione dei dati personali (data breach) ovvero, che, pur non avendo un impatto diretto su di essi, possa comunque esporli a rischi di violazione (p.es.accessi abusivi al sistema informativo, azione di malware sul sistema informatico…).

NOTIFICA: si intende la notifica che deve essere fatta all'Autorità di Controllo al verificarsi delle circostanze previste dall'art. 33.

NOTIZIA: si intende l'informativa di un incidente o sospetto incidente che viene fornita, con qualsiasi mezzo, ad un responsabile di struttura.

VIOLAZIONE DEI DATI PERSONALI: si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

E. AZIONI

E.1. Organizzazione

Il titolare individua un responsabile per le violazioni cui assegna il compito di ricevere le segnalazioni, valutarne la portata, compilare il registro delle violazioni e, se del caso, predisporre la notifica e la comunicazione in tempo utile.

Il titolare si assicura che:

- il flusso informativo delle violazioni sia definito, assegnato, noto, verificato e mantenuto aggiornato;

- che i passaggi siano tracciati temporalmente e che siano identificabili gli autori.

E.2. Formazione

Il titolare si assicura che nei programmi di formazione del personale sia data informazione sui concetti della violazione dei dati personali, sui principi e gli obiettivi adottati dal titolare, su questa procedura, sulla persona del responsabile delle violazioni e sulle conseguenze del mancato rispetto delle regole e delle norme.

E.3. Comunicazione

Il titolare si assicura che sia data adeguata informazione, riguardo i compiti ed i contatti del responsabile per le violazioni dei dati personali, ai dipendenti, ai fornitori e a tutti coloro che trattano dati personali sotto la sua responsabilità.

Il titolare si assicura che i responsabili del trattamento che operano per suo compito siano obbligati a trasmettere la segnalazione di violazione il più rapidamente possibile, prevedendo anche misure correttive in caso di mancato rispetto.

E.4. Rilevamento incidente

Chiunque, persona autorizzata al trattamento, o, responsabile del trattamento, operando per conto di AO Terni, è testimone o viene a conoscenza di un incidente o di un sospetto incidente che interessa dati personali, ha il dovere di informare immediatamente, attraverso la modalità di comunicazione dedicata (email, sms, allarme web) il responsabile per le violazioni.

E.5. Registrazione

Il Responsabile per le Violazioni immediatamente ne accerta la fondatezza e, in caso positivo:

E.5.1 registra subito la segnalazione nel registro delle violazioni;

E.5.2. raccoglie tutte le informazioni occorrenti.

E.6. Valutazione

Il Responsabile per le Violazioni valuta senza indugio la severità della violazione secondo la scala di valutazione (Appendice A).

E.7. Violazione che non comporta rischi per i diritti e le libertà delle persone fisiche.

Il Responsabile per le Violazioni, chiude l'incidente, mettendo a disposizione le informazioni raccolte al fine di individuare eventuali responsabilità e migliorare il sistema di protezione dei dati.

E.8. Violazione che comporta rischi per i diritti e le libertà delle persone fisiche.

Il Responsabile per le Violazioni, senza indugio:

E.8.1. ne da immediata comunicazione al delegato del titolare, fornendo tutte le informazioni necessarie, affinché proceda alla notifica all'Autorità di Controllo entro le 72 ore dalla scoperta della violazione;

E.8.2. informa l'eventuale Responsabile per la Protezione dei Dati.

E.9. Violazione che comporta un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Responsabile per le Violazioni, senza indugio:

E.9.1. ne da immediata comunicazione al delegato del titolare, fornendo tutte le informazioni necessarie, affinché proceda alla comunicazione agli interessati ai sensi dell'art. 34 del Regolamento;

E.9.2. informa l'eventuale Responsabile per la Protezione dei Dati.

E.10 Ritardo nella notifica e/o comunicazione.

Nel caso in cui non dovesse essere rispettato il termine di 72 ore per la notifica all'Autorità di Controllo, il Responsabile per le Violazioni, ovvero il Responsabile per la Protezione dei Dati Personali, se presente, raccolgono le informazioni riguardo alle cause del ritardo e le trasmettono immediatamente al delegato del titolare onde permettergli di fare la notifica prevista dall'art. 33 corredandola delle ragioni del ritardo.

6. REVISIONI

Questa procedura è mantenuta aggiornata dal responsabile per la privacy che ne cura la diffusione ed il controllo all'interno dell'Ente.

APPENDICE A

ELEMENTO DI VALUTAZIONE	BASSO	MEDIO	ALTO
Natura dei dati personali	• Personali	• Particolari • Giudiziali	• Sanitari • Sessuali
Sensibilità dei dati personali	• Anagrafici	• Bancari • Reddito	• Carte di credito • Documenti di identificazione • Credenziali di accesso • Iscrizioni
Volume dei dati personali	1	2 - 4	5>
Facilità di identificazione degli interessati	Alta difficoltà (pseudonimizzazione)	Media difficoltà (identificativi indiretti, p.es. PIVA, CF, TARGA)	Bassa difficoltà (identificativi)

ELEMENTO DI VALUTAZIONE	BASSO	MEDIO	ALTO
Severità delle conseguenze per gli interessati	Gli interessati non subiscono alcuna conseguenza, oppure piccoli inconvenienti facilmente superabili senza problemi o con piccoli costi.	Gli interessati possono subire conseguenze significative che possono essere superate con serie difficoltà.	Gli interessati possono subire conseguenze difficilmente superabili, o danni irreversibili, o irrisarcibili.
Specifiche caratteristiche degli interessati	Adulti	Anziani	Minori Disabili Incapaci
Il numero degli interessati trattati	500 <	>500 - 2.000<	> 2.000

APPENDICE B

AZIONE	RESPONSABILITÀ	AUTORITÀ	COLLABORAZIONE	INFORMAZIONE
FORMAZIONE	Privacy Manager	Amministratore Unico		
COMUNICAZIONE	Chiunque	Responsabile Gerarchico		
RILEVAMENTO	Chiunque	Responsabile Gerarchico		
REGISTRAZIONE	Responsabile per le Violazioni	Privacy Manager		
VALUTAZIONE	Responsabile per le Violazioni	Privacy Manager	DPO	
CHIUSURA	Responsabile per le Violazioni	Privacy Manager		DPO
NOTIFICA	Delegato del Titolare	Amministratore Unico		DPO
COMUNICAZIONE	Delegato del Titolare	Amministratore Unico		DPO

AZIONE	RESPONSABILITÀ	AUTORITÀ	COLLABORAZIONE	INFORMAZIONE
VIGILANZA	DPO	DPO		Amministratore Unico