PROTOCOLLO PRIVACY

Regolamento UE 2016/679

DATA

BREACH

ORDINE PROVINCIALE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI MODENA

REV	Data revisione	Oggetto	Responsabile	Firma
00		Prima approvazione	Il Legale Rappresentante p.t.	

Sommario

1.Scopo e campo di applicazione

Scopo del presente protocollo è quello di gestire eventuali violazioni dei dati personali, ai sensi degli articoli 33 e 34 Regolamento UE 679/2016 (GDPR), a tutela delle persone interessate al trattamento e dei loro dati personali.

Il mancato rispetto del presente protocollo può comportare l'applicazione delle sanzioni di cui all'articolo 83 GDPR

2.Funzioni interessate

Le funzioni interessate sono il Titolare, i dipendenti e i professionisti tutti che operano all'interno della struttura, il Responsabile per la protezione dei dati personali (DPO) nonché Responsabili esterni che trattano i dati personali per conto del Titolare.

3.Protocolli e procedure collegate

Tutti protocolli eventualmente adottati in materia di protezione dei dati personali.

4.Normativa collegata

- Direttiva 2002/58 e-privacy e s.m.i. e D.lgs. 28 maggio 2002, n. 69;
- Regolamento UE n. 611/2013, recante misure applicabili alla notifica delle violazioni di dati personali a norma della Direttiva 2002/58;
- D.lgs. 196/2003 e s.m.i.;
- Regolamento UE 23 luglio 2014, n. 910 c.d. eIDAS in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche;
- Direttiva 2016/1148 NIS, Network and Information Security.

Garante Italiano:

- Provv. 4.4.2013 n. 161 [doc. web 2388260] in materia di società telefoniche e internet provider, secondo cui la comunicazione al Garante deve essere effettuata entro 24 ore dalla conoscenza dell'evento in maniera sommaria ed entro 3 giorni in forma dettagliata, e la comunicazione all'interessato contraente e alle altre persone coinvolte entro 3 giorni, nei casi previsti;
- Provv. 12.11.2014 n. 513 [doc. web 3556992] in materia di biometria, secondo cui la comunicazione al Garante deve essere effettuata entro 24 ore dalla conoscenza della violazione;
- Provv. 4.6.2015 n. 331 [doc. web 4084632] in materia di dossier sanitario elettronico, secondo cui la comunicazione al Garante deve avvenire entro 48 ore dalla conoscenza della violazione;
- Provv. 2.7.2015 n. 393 [doc. web 4129029] in materia di Pubblica Amministrazione, secondo cui la comunicazione al Garante deve avvenire entro 48 ore dalla conoscenza della violazione.

5.Obbligo di segnalazione nei confronti del Titolare del trattamento

Chiunque venga a conoscenza, ovvero abbia il sospetto o la consapevolezza di una violazione dei dati personali trattati dal Titolare, deve darne tempestiva comunicazione al Titolare stesso e al Responsabile per la protezione dei dati personali (DPO).

Per violazione dei dati personali (Data Breach) deve intendersi "*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*".

Pertanto si ha:

i. Distruzione: quando i dati trattati non esistono più o non sono più nel formato utilizzato e utile per il Titolare del trattamento;
ii. Perdita: quando il Titolare non ha più il controllo, l'accesso o il possesso dei dati trattati;
iii. Divulgazione: quando avviene la comunicazione, trasmissione dei dati personali a soggetti non preventivamente identificati tra i destinatari dei dati personali nell'informativa trasmessa agli Interessati, nemmeno per appartenenza ad una determinata categoria;
iv. Accesso: quando vi è un accesso ai dati personali da parte di soggetti non autorizzati, in quanto non preventivamente individuati quali Incaricati o Responsabili del trattamento.

La segnalazione deve essere effettuata per iscritto, secondo le modalità di seguito indicate, ed inoltrata con i canali appositamente creati tra loro alternativi:

- e-mail del Titolare ed e-mail del DPO;

Il contenuto minimo della segnalazione deve essere il seguente:

i. Dati del segnalante:
   - Nome e cognome del segnalante;
   - Qualifica servizio attuale;
   - Ufficio e incarico attuale;
   - Qualifica servizio all'epoca del fatto;
   - Ufficio e incarico all'epoca del fatto;
   - Telefono ed e-mail.
ii. Dati e informazione della violazione dei dati:
   - Periodo/data in cui si è verificato il fatto e in cui ne è venuto a conoscenza, se differente;
   - Luogo in cui si è verificato il fatto, se conosciuto;
   - Soggetto o soggetti che hanno commesso il fatto (nome, cognome, qualifica), se noti;
   - Eventuali soggetti privati coinvolti, se noti;
   - Breve descrizione della violazione con produzione di eventuali evidenze documentali;
   - Modalità con cui il segnalante è venuto a conoscenza del fatto;
   - Eventuali altri soggetti che possono riferire sul fatto (nome, cognome, qualifica, recapiti);
   - Area/settore/ufficio in cui può essere stato commesso il fatto, se avvenuto internamente alla struttura.

5.1 Tutela del segnalante

Si specifica al riguardo che è fatto espresso divieto di porre in essere atti di ritorsione, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

L'eventuale adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni devono essere denunciati all'Ispettorato Nazionale del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche eventualmente dall'organizzazione sindacale indicata dal medesimo.

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.

È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamento, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

La violazione delle misure di tutela del segnalante e le segnalazioni effettuate con dolo o colpa grave che si rivelano infondate devono essere sanzionate conformemente al sistema disciplinare adottato.

5.2 Obbligo di segnalazione da parte dei Responsabili esterni del trattamento

I rapporti tra il Titolare e i Responsabili esterni del trattamento devono essere disciplinati da un contratto, o altro atto avente forza di legge, che disciplini, tra gli altri, l'obbligo di notificazione della violazione nei confronti del Titolare stesso.

Il Responsabile del trattamento deve notificare, immediatamente e senza indebito ritardo, nel momento in cui ne viene a conoscenza ovvero se ne ha il sospetto o la consapevolezza, e comunque nel termine di 48 (quarantotto ore) la violazione verificatesi, affinché il Titolare possa affrontare la violazione e determinare se è tenuto o meno a notificare la stessa all'Autorità di controllo ex art. 33 GDPR, e a comunicarla alle persone interessate ex art. 34 GDPR.

Le ulteriori informazioni sulla violazione dovranno essere trasmesse dal Responsabile al Titolare del Trattamento man mano che queste diventano disponibili.

Il Responsabile può effettuare le notifiche per conto del Titolare del trattamento esclusivamente previa autorizzazione scritta facente parte del contratto o dell'altro atto avente forza di legge sottoscritto tra le parti.

La segnalazione deve essere effettuata per iscritto, secondo le modalità di seguito indicate, ed inoltrata con i canali appositamente creati:

- e-mail del Titolare ed e-mail del DPO.

Il contenuto minimo della segnalazione deve essere il seguente:

- Natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo degli interessati in questione nonché le categorie e il numero approssimativo di registrazione dei dati personali in questione;
- Periodo/data in cui si è verificato il fatto e in cui ne è venuto a conoscenza, se differente;
- Luogo in cui si è verificato il fatto, se conosciuto;
- Modalità con cui il segnalante è venuto a conoscenza del fatto;
- Breve descrizione della violazione con produzione di eventuali evidenze documentali;
- Probabili conseguenze della violazione dei dati personali;
- Misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- Soggetto o soggetti che hanno commesso il fatto (nome, cognome, qualifica), se noti;

- Eventuali soggetti privati coinvolti, se noti;
- Eventuali altri soggetti che possono riferire sul fatto (nome, cognome, qualifica, recapiti);
- Area/settore/ufficio in cui può essere stato commesso il fatto, se avvenuto internamente alla struttura.

La mancata o ritardata notificazione, senza alcuna legittima giustificazione, può essere prevista quale causa di risoluzione espressa del contratto.

Tale paragrafo si applica anche nel caso in cui la Società sia nominata Responsabile esterno del trattamento da altri Titolari e debba pertanto, a sua volta, notificare eventuali violazioni dei dati ai rispettivi Titolari.

6.Modalità operative di gestione del Data Breach

Il Titolare del trattamento e il DPO o altra funzione a ciò incaricata valutano, con tempestività, la violazione dei dati intercorsa, anche a seguito della segnalazione effettuata, e compilano il file, Registro delle violazioni, inserito all'interno dei Registri dei Dati.

- **Comunicazione** dell'avvenuta presa in carico della segnalazione al segnalante, al Responsabile esterno e al Titolare, salvo che il Titolare non abbia autonomamente preso conoscenza della violazione. Congiuntamente all'avviso di presa in carico, il segnalante e il Responsabile esterno devono essere avvisati della possibilità di essere ricontattati per acquisire eventuali elementi utili alla fase istruttoria e dell'obbligo di comunicare ulteriori informazioni ed elementi di cui vengano a conoscenza successivamente alla segnalazione iniziale, al fine di integrare / aggiornare i fatti oggetto della segnalazione iniziale.

- **Istruttoria:** successivamente alla avvenuta presa in carico della segnalazione, il Titolare o il DPO o altra funzione incaricata, deve intraprendere un breve periodo di indagine al fine di verificare la fondatezza della violazione, effettuare indagini, raccogliere prove e valutare il rischio al fine di verificare l'obbligo di notifica nei confronti dell'Autorità e di comunicazione nei confronti dei soggetti Interessati, anche mediante l'ausilio di soggetti esterni.
  Qualora il Titolare o il DPO o altra funzione a ciò incaricata, non sia in grado di acquisire elementi utili per verificare la sussistenza del rischio per i diritti e le libertà delle persone fisiche e gli elementi necessari per effettuare la notifica entro il termine di 72 (settantadue) ore dalla presa di conoscenza della violazione, deve procedere immediatamente alla notifica nei confronti dell'Autorità di cui al punto seguente, al fine di garantire il rispetto dei termini legali, riservandosi di fornire successivamente le informazioni concernenti la notifica stessa. Qualora si ritenga che la predetta violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione andrà effettuata anche nei confronti degli Interessati, come indicato *infra.*

- **La notifica al Garante per la privacy**
  Al fine di valutare se la violazione comporti la necessità di effettuare la notifica al Garante per la privacy, il Titolare o il DPO o altra funzione a ciò incaricata, compila il file contenente le domande redatte da Enisa, nel documento denominato "Raccomandazioni per la valutazione del grado di gravità del data breach", del dicembre 2013, allegato alla presente.
  All'esito di tale valutazione, il Titolare o il DPO o altra funzione a ciò incaricata, procede con la notifica al Garante per la privacy, qualora la violazione comporti un rischio per i diritti e le libertà delle persone fisiche. Qualora, all'esito della valutazione effettuata, risulti che la violazione non

comporta un rischio per i diritti e le libertà delle persone fisiche, essa andrà annotata sul Registro delle Violazioni e non si procedere alla notifica. Nell'ipotesi in cui, all'esito della valutazione effettuata, risulti che il rischio per i diritti e le libertà delle persone fisiche è elevato, si procederà anche con la comunicazione ai medesimi Interessati, come indicato *infra.*

La notifica al Garante viene effettuata entro e non oltre il termine di 72 (settantadue) ore dalla presa di conoscenza, mediante la compilazione del modulo reperibile presso il sito del Garante.
In ogni caso la notifica deve, almeno:

a) descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di Interessati, nonché le categorie e il numero approssimativo di registrazione dei dati personali in questione;
b) comunicare il nome e i dettagli di contatto del DPO o altra funzione a ciò incaricata, presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Notifica in fasi: Qualora il Titolare o il DPO o altra funzione a ciò incaricata, non sia in possesso di tutte le informazioni necessarie in merito alla violazione, nel termine delle 72 ore dalla presa di coscienza dello stesso, in quanto i dettagli non sono disponibili in questo arco temporale, deve informare il Garante e fornire le ragioni del ritardo congiuntamente alla notifica, che deve comunque avvenire nel termine di legge prescritto.
Il Titolare o il DPO o altra funzione a ciò incaricata, anche previo accordo con l'Autorità, dovrà compiere ulteriori indagini e follow-up e fornire ulteriori informazioni.
Si precisa che a seguito delle ulteriori indagini potrebbe emergere il fatto che non sussistono gli estremi per la notifica nei confronti degli Interessati e della stessa Autorità, ciò non comporta alcuna sanzione qualora sia stata già effettuata.

Notifiche ritardate: qualora la notifica all'Autorità di controllo non venga effettuata nel termine di 72 ore, essa deve essere accompagnata dai motivi del ritardo.

Notifica raggruppata: il Titolare, il DPO o altra funzione a ciò incaricata, può effettuare una notifica raggruppata al Garante in caso di violazioni di riservatezza multiple e simili, ovvero che riguardano lo stesso tipo di dati personali violati nello stesso modo e in un lasso di tempo relativamente breve.

- **L'Autorità di controllo competente**

La notifica deve essere effettuata nei confronti dell'Autorità di controllo, ovvero del Garante dello stato membro in cui sorge lo stabilimento del Titolare interessato alla violazione di sicurezza, pertanto al Garante Italiano.
Qualora la violazione incida sui dati personali delle persone fisiche in più di uno Stato membro e la notifica è richiesta, il Titolare del trattamento, il DPO o la funzione a ciò incaricata, deve notificare all'Autorità di controllo principale. Pertanto, nel redigere il proprio piano di risposta alle violazioni, un Titolare del trattamento deve effettuare una valutazione in merito a chi sia l'Autorità principale cui notificare la violazione, al fine di reagire prontamente a una violazione e di adempiere ai propri obblighi.

Se il Titolare del trattamento ha dubbi sull'identità dell'Autorità di controllo capofila deve, come minimo, notificare all'Autorità di controllo locale dove è avvenuta la violazione. Il Titolare può anche segnalare, a sua discrezione, l'incidente a un'Autorità di controllo che non è la sua autorità capofila, ad esempio se il Titolare sa che le persone nell'altro Stato membro sono interessate dalla violazione. Se il Titolare sceglie di notificare solo all'Autorità di controllo capofila, tuttavia, deve indicare, se del caso, che la violazione coinvolge stabilimenti situati in altri Stati membri e in quali Stati membri le persone interessate potrebbero essere state interessate dalla violazione.

- **La comunicazione agli Interessati**

Qualora a seguito dell'istruttoria venga rilevato un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, il DPO o la funzione a ciò incaricata, comunica la violazione all'Interessato immediatamente e senza indebito ritardo.

La comunicazione deve avvenire con un linguaggio semplice e chiaro, nella lingua madre del soggetto destinatario, mediante messaggistica diretta (e-mail, sms), banner dei siti web o notifiche, comunicazioni postali e pubblicità di rilievo nei mezzi di stampa, e deve almeno:

a. descrivere la natura della violazione dei dati personali;
b. comunicare il nome e i dettagli di contatto del DPO o di altra funzione a ciò incaricata, presso cui ottenere più informazioni;
c. descrivere le probabili conseguenze della violazione dei dati personali;
d. descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

In caso di dubbi, il Titolare deve contattare e consultare il Garante per chiedere consiglio se informare gli Interessati e con quali modalità effettuare la stessa comunicazione.

Il Titolare deve fornire consulenza specifica agli Interessati al fine di proteggerli da possibili ulteriori conseguenze negative:

- qualora, successivamente alla notifica effettuata al Garante, il Titolare abbia ricevuto un parere sulla gestione della violazione e sulla riduzione dell'impatto;
- su richiesta dell'Interessato.

La comunicazione non deve essere effettuata, qualora:

a. il Titolare del trattamento abbia messo in atto le misure tecniche e organizzative adeguate di protezione, e tali misure siano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b. il Titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati. In tal caso è necessario tenere in debito conto le possibili conseguenze di eventuali violazioni della riservatezza a seconda della natura dei dati in questione;
c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si deve procedere a una comunicazione pubblica o ad altra misura simile, tramite la quale gli interessati siano informati con analoga efficacia.

Il Titolare del trattamento deve essere in grado di dimostrare all'Autorità di controllo di soddisfare una o più di queste condizioni.

Va tenuto presente che, sebbene la comunicazione inizialmente non sia necessaria qualora non si ravvisi un rischio per i diritti e libertà delle persone fisiche, questo può cambiare nel tempo e il rischio deve essere rivalutato.

Se il Titolare decide di non comunicare la violazione agli Interessati, Egli deve comunque effettuarla se richiesto dall'Autorità di controllo, poiché potrebbe comportare un rischio alto per le persone.

7.Obbligo di documentazione del Data Breach

Il Titolare, il DPO o altra funzione a ciò incaricata, deve documentare tutte le violazioni dei dati personali nel file Registro delle opposizioni contenuto nel Registro Protezioni Dati e procedere alla corretta e puntuale compilazione del medesimo.

La documentazione deve riguardare anche le violazioni dei dati personali delle quali il Titolare ha deciso di non effettuare la notifica all'Autorità di controllo e la comunicazione agli interessati ai sensi degli artt. 33 e 34 GDPR, qualora a seguito della fase istruttoria si sia rilevato che le stesse non presentassero un probabile rischio o un alto rischio per i diritti e le libertà le libertà delle persone fisiche, a seconda del caso.

La documentazione deve essere resa accessibile all'Autorità di controllo per permette di verificare il rispetto delle disposizioni.

La mancata tenuta del Registro delle violazioni può comportare l'irrogazione di sanzioni.

8.Allegati

1. Documento per la valutazione del grado di gravità del rischio per i diritti e le libertà delle persone fisiche a seguito di Data Breach.