Allegato 10 – Segnalazione data breach

Modello per la raccolta di informazioni sulla violazione dei dati personali

(artt.4, 33, 34 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Sez. A - Dati del soggetto segnalante

Cognome: _____ Nome:_____
E-mail:_____
Recapito telefonico per eventuali comunicazioni:_____
Funzione:_____

Sez. B -Titolare del Trattamento

Denominazione[1]: Ordine provinciale dei Medici Chirurghi e degli Odontoiatri di

Codice Fiscale:
Indirizzo:
PEC:

Sez. B1- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile del trattamento[2] rappresentante del titolare non stabilito nell'Ue)

Denominazione: _____
Codice Fiscale/P.IVA_____(indicare se Soggetto privo di C.F./P.IVA)
Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Denominazione: _____
Codice Fiscale/P.IVA_____(indicare se Soggetto privo di C.F./P.IVA)
Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Denominazione: _____
Codice Fiscale/P.IVA_____(indicare se Soggetto privo di C.F./P.IVA)
Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

[1] Indicare nome e cognome nel caso di persona fisica.
[2] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4.

Sez. C - Informazioni di sintesi sulla violazione

Indicare quando è avvenuta la violazione

☐ Il _____

☐ Dal _____ (la violazione è ancora in corso)

☐ Dal _____ al _____

☐ In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

1. Breve descrizione della violazione

2. Natura della violazione

☐ a) Diffusione/accesso non autorizzato o accidentale [3]

☐ b) Modifica non autorizzata o accidentale [4]

☐ c) Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale [5]

3. Causa della violazione

☐ Azione intenzionale interna

☐ Azione accidentale interna

☐ Azione intenzionale esterna

☐ Azione accidentale sterna

☐ Sconosciuta

☐ Altro (specificare)

---

3. Perdita di confidenzialità
4. Perdita di integrità
5. Perdita di disponibilità

4. Categorie di dati personali oggetto di violazione

- ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
- ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
- ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, altro…)
- ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
- ☐ Dati di profilazione (elaborazione automatizzata dei dati personali)
- ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
- ☐ Dati di localizzazione
- ☐ Dati che rivelino l'origine razziale etnica
- ☐ Dati che rivelino opinioni politiche
- ☐ Dati che rivelino convinzioni religiose o filosofiche
- ☐ Dati che rivelino l'appartenenza sindacale
- ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
- ☐ Dati relativi alla salute
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Categorie ancora non determinate
- ☐ Altro

5. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[6]

[6] Ad esempio, numero di referti, numero di record di un database, numero di transazioni registrate.

☐ N. _____
☐ Circa n. _____
☐ Un Numero (ancora) non definito di dati

6. Categorie di interessati coinvolti nella violazione

☐ Dipendenti/Consulenti ecc.
☐ Utenti in genere
☐ Iscritti all'Ordine
☐ Soggetti che ricoprono incarichi istituzionali
☐ Beneficiari
☐ Pazienti
☐ Minori
☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
☐ Categorie ancora non determinate
☐ Altro (specificare)

☐ Eventuali ulteriori dettagli circa le categorie di interessati

7. Numero (anche approssimativo) di interessati coinvolti nella violazione

☐ N. _____ interessati
☐ Circa n. _____ interessati
☐ Un numero (ancora) sconosciuto di interessati

Sez. D - Informazioni di dettaglio sulla violazione[7]

1. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

☐ Computer

[7] Segue punto 1, 2 e 3 della sez. C.

☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di file
☐ Strumento di back up
☐ Rete
☐ Altro:

2. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[8]

a) Misure organizzative:

☐ Nomina per iscritto personale
☐ Istruzioni per il trattamento
☐ Formazione del personale
☐ Accesso controllato
☐ Armadi chiusi
☐ Procedura modifica credenziali
☐ Policy di Ateneo

b) Misure tecniche:

☐ Autenticazione
☐ Autorizzazione
☐ Cifratura dei dati
☐ Separazione
☐ Firewall
☐ Antivirus
☐ Business continuity
☐ Disaster recovery
☐ Intrusion detection
☐ Vulnerability assessment/penetration test

Sez. E – Misure adottate a seguito della violazione

[8] Indicare le misure in essere al momento della violazione.

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[9]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

[9] Nella descrizione distinguere le misure adottate da quelle in corso di adozione.