Data Breach Policy

Procedura di notifica di violazione dei dati personali

Data di ultima revisione della policy: 07/11/2018

Net4market - CSAmed s.r.l.

Corso G. Matteotti 15
26100 Cremona IT

Tel. +39 0372 801730
Fax +39 0372 801740
C.F. e P.IVA 02362600344

www.net4market.com
info@net4market.com

INDICE

1. PREMESSE 3
2. SCOPO 3
3. COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) 3
4. A CHI SONO RIVOLTE QUESTE PROCEDURE? 4
5. A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE 4
6. GESTIONE COMUNICAZIONE DI DATA BREACHES 4
7. GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI 5
Step 1: Identificazione e indagine preliminare 5
Step 2: Contenimento, Recovery e risk assessment 5
Step 3: Eventuale notifica all'Autorità Garante competente 6
Step 4: Eventuale comunicazione agli interessati 6
Step 5: Documentazione della violazione 6

PREMESSE

Net4market – CSAmed s.r.l, ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ateneo e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.
Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo a Net4market – CSAmed s.r.l di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni dei dati personali trattati da Net4market – CSAmed s.r.l in qualità di Titolare del trattamento (di seguito "**Titolare del trattamento**"). Queste procedure sono ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento.
Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del **Titolare del trattamento** (meglio descritti al punto 5 della presente procedura) quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati Destinatari interni);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati Destinatari esterni);

  di seguito, genericamente denominati "Destinatari".

Tutti i Destinatari devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.
Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

A QUALI TIPI DI DATI SI RIFERISCONO QUESTE PROCEDURE

Queste procedure si riferiscono a:

- dati personali trattati "da "e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema aziendale.

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.

GESTIONE COMUNICAZIONE DI DATA BREACHES

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.
In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.
Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente **informare dell'incidente il superiore gerarchico** il quale si occuperà, con il supporto dei Destinatari stessi, di informare il Titolare del trattamento o un suo delegato mediante la compilazione dell'**Allegato A – Modulo di comunicazione interna di Data Breach** da inviare a mezzo mail all'indirizzo privacy@net4market.com

GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti quattro step:

Step 1: Identificazione e indagine preliminare
Step 2: Contenimento, recovery e risk assessment
Step 3: Eventuale notifica all'Autorità Garante
Step 4: Eventuale comunicazione agli interessati
Step 5: Documentazione della violazione

Step 1: Identificazione e indagine preliminare

L'**Allegato A**, debitamente compilato, permetterà al Titolare del trattamento o un suo delegato, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2) e con il coinvolgimento del DPO.
Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o un suo delegato **dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Ufficio IT o un suo delegato in caso di assenza.**
Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A, quali:

- la data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:
- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento e il DPO valuteranno la gravità della violazione utilizzando l'**Allegato B - Modulo di valutazione del Rischio connesso al Data Breach** che dovrà essere esaminato unitamente all'Allegato A, tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR.
Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio *semplice*, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio *elevato*.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, **Net4market – CSAmed s.r.l** dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.
Pertanto, il Titolare del trattamento e il DPO individueranno l'Autorità di Controllo competente sulla base delle informative e/o della valutazione d'impatto sulla protezione dei dati già in essere presso **Net4market – CSAmed s.r.l** in relazione ai dati oggetto di violazione (in mancanza di tale documentazione che abbia preventivamente individuato l'Autorità Garante competente, la stessa sarà da individuare in quella dello Stato in cui è ubicato lo stabilimento principale o lo stabilimento unico del Titolare del trattamento, anche per i trattamenti transfrontalieri eventualmente effettuati).

Una volta determinata l'Autorità di Controllo competente, il Titolare del trattamento e il DPO individueranno la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, **Net4market – CSAmed s.r.l** dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare del trattamento o da un suo delegato e il DPO dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (DPO);
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o da un suo delegato e il DPO dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A Net4market – CSAMed s.r.l sarà tenuta a documentarlo.
Tale documentazione sarà affidata al Titolare del trattamento o da un suo delegato con l'ausilio del Responsabile dell'Ufficio IT (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta dell'**Allegato C Registro dei Data Breach**, secondo le informazioni ivi riportate:

(i) n. violazione;
(ii) data violazione;
(iii) natura della violazione;
(iv) categoria di interessati;
(v) categoria di dati personali coinvolti;

(vi) numero approssimativo di registrazioni dei dati personali;
(vii) conseguenze della violazione;
(viii) contromisure adottate;
(ix) se sia stata effettuata notifica all'Autorità Garante Privacy;
(x) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente il Suo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email: privacy@net4market.com

S1 Segnalazione

ID N^/anno	
Data:	
Segnalante:	
Modalità di comunicazione	
Segnalazione:	
Allegati eventuali (es. mail)	
Membri presenti del team	
Decisione (Se procedere S2 se no S6)	

S2 Team crisi - conseguenze dell'evento

N^ interessati e/o %/N^ dati coinvolti:	
Dati personali:	
Portata dell'evento:	
Arco temporale che interessa l'evento:	
Formato dati (carteceo/elettronico)	
Eventuali azioni per contenre effetti dell'evento	
Data:	
Violazione:	Sì

S4 Titolare: NOTIFICA all'autorità di controllo dello stato in cui è avvenuta la violazione

Documento di notifica:	
Modalità di invio	
Data e ora:	

S5 Titolare: COMUNICAZIONE agli interessati coinvolti

Comunicazione obbligatoria si /no se no motivazione	
Documento di comunicazione:	
Data e ora:	

S6 Decisione a non procedere con la segnalazione

Data:	
Motivazione	
Membri presenti del team	
Comunicazione a TdT	
Eventuale AC? (vai a S8)	

S7 Trattamento

Data:	
Trattamento	
Responsabile del trattamento	
Tempi di effettuazione	
Comunicazione a TdT	
Esito ed azioni in caso di esito negativo	

S8 Azione correttiva

Data:	
Azione correttiva	
Responsabile della AC	
Tempi di effettuazione	
Comunicazione a TdT	
Valutazione di efficacia ed azioni in caso di esito negativo	
Eventuale aggiornamento AdR/PIA	
Eventuale aggiornamento documentazione	

S9 Decisione di interruzione della analisi da parte del Titolare

Data:	
Motivazione	
Membri presenti del team	
Comunicazione in data certa del	
Allegato	

net4market

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

	S3 Team crisi - analisi del rischio		Valore del rischio
1	Violazione di riservatezza	da 1 a 4 + descrizione	1
2	Violazione di disponibilità	da 1 a 4 + descrizione	1
3	Violazione di integrità	da 1 a 4 + descrizione	1
4	Natura dei dati violati: sanitari	No / Sì + descrizione	
5	Natura dei dati violati: doc. d'identità	No / Sì + descrizione	
6	Natura dei dati violati: numeri carte di credito	No / Sì + descrizione	
7	Natura dei dati violati: reddito, fatturato	No / Sì + descrizione	
8	Natura dei dati violati: brevetti, strategie di marketing, segreti professionali	No / Sì + descrizione	
9	Natura dei dati violati altri (es biometria) _____	No / Sì + descrizione	
10	Facilità d'identificazione degli interessati	No / Sì + descrizione	
11	Gravità delle conseguenze sugli individui in termini di danni fisici, materiali ed immateriali (approfondimento S2)	No / Sì + descrizione	
12	Speciali caratteristiche dei dati violati: dati sanitari-giudiziari	No / Sì + descrizione	
13	Speciali caratteristiche dei dati violati: dati sui minori	No / Sì + descrizione	
14	Speciali caratteristiche dei dati violati: dati sulla localizzazione dell'interessato	No / Sì + descrizione	
15	Speciali caratteristiche dei dati violati: dati sulle abitudini/preferenze dell'interessato	No / Sì + descrizione	
16	Numero di individui interessati: violazione massiccia o individuale anche in base all'universo di riferimento	No / Sì + descrizione	
17	Criptazione dei dati (con criptazione valore 0)	No / Sì + descrizione	
18	Esistenza di copie dei dati (con esistenza copia valore 0)	No / Sì + descrizione	

Data:		TOTALE = indicare un valore da 3 a 27	3
		VALORE DATA BREACH = indicare da A) a D)	

Il risultato del calcolo del rischio deve essere interpretato come segue, considerando che, in base ai criteri assegnati il valore minimo è 3 ed il massimo è 27:

A. Valore data breach - da 1 - 3 = nessun rischio – MISURE: non fare NOTIFICA e COMUNICAZIONE e valutare eventuale AC vedi S8 nel MODULO Gestione del Data Breach
B. Valore data breach - da 3 a 8 = rischio - MISURE: non fare NOTIFICA e COMUNICAZIONE all'interessato , effettuare il trattamento dell'evento vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach;
C. Valore data breach - da 9 a 15 = rischio - MISURE: fare NOTIFICA, non fare la COMUNICAZIONE all'interessato , effettuare il trattamento dell'evento vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach;
D. Valore data breach – oltre 15 MISURE:= rischio che implica: quanto previsto al caso 3 ed anche la COMUNICAZIONE obbligatoria agli interessati coinvolti