ALLEGATO 3

Disciplinare d'intervento del personale dipendente - violazione di sicurezza dei dati personali -

Titolare del Trattamento

Il Titolare del trattamento è l'Università degli Studi del Sannio, Piazza Guerrazzi, 1 - 82100 Benevento (BN), PEC: amministrazione@cert.unisannio.it , Mail:segreteria.rettore@unisannio.it

Responsabile della protezione dati

Il Responsabile della protezione dei dati è raggiungibile al seguente recapito: dpo@unisannio.it

Premesse

L'Università degli Studi del Sannio, 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 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).

Il presente regolamento ha la finalità di consentire l'individuazione di una violazione di sicurezza dei dati personali e la valutazione dei rischi che possono determinare l'obbligo di notifica, in particolare, la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica.

A titolo d'esempio si elenca: perdita del controllo dei dati personali; limitazione dei diritti; discriminazione; furto o usurpazione di identità; perdite finanziarie; decifratura non autorizzata della pseudonimizzazione; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo per la persona interessata.

La presente procedura si applica a tutte le informazioni personali che sono raccolte o gestite o comunque trattate dall'Università degli Studi del Sannio, siano esse contenute su dispositivi elettronici, accessibili via rete o web, contenute su dispositivi mobili o portatili ovvero su supporti cartacei.

La presente procedura è ad integrazione delle procedure adottate dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

Fatte salve le disposizioni previste dagli artt. 5, 6 e 8 (comunicazione e doveri), al fine rendere agevole e tempestiva la comunicazione di una violazione dei dati, poiché il processo di gestione dell'evento può avere diverse varianti ed aspetti non definibili a priori, non si fa vincolo di seguire scrupolosamente le indicazioni procedurali contenute nel presente documento.

Il disciplinare ha lo scopo di indicare una possibile metodologia per affrontare al meglio ed assolvere i compiti che scaturiscono dalle norme in materia di violazione dei dati sotto la responsabilità del Titolare.

Allo stesso modo non si fa obbligo di utilizzare, nell'imminenza dell'evento, il modulo predisposto per la raccolta delle informazioni.

Art. 1

Oggetto

Il presente disciplinare stabilisce le regole e le procedure da mettere in atto in caso di violazione dei dati personali.

Art. 2

Definizioni

Ai fini del presente disciplinare si intende per:

Violazione dei dati personali (c.d. *Data Breach*): 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;
Dato personale: 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;
Distruzione dei dati: operazione che non consente il recupero dei dati e che determina la cancellazione dei dati o la non esistenza in una forma che sia di qualche utilità per il titolare del trattamento;
Perdita dei dati: i dati potrebbero esistere, ma il Titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso;
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Art. 3
Identificazione dell'evento

La violazione di dati personali può avvenire sia per eventi accidentali che per eventi volontari.
Tra gli eventi accidentali rientrano gli eventi avvenuti per:
• distruzione accidentale di documenti (incendio o allagamento dei locali dove sono presenti archivi cartacei);
• distruzione per errore di documenti originali, senza avere il possesso di una eventuale copia;
• smarrimento di documenti;
• fornitura involontaria di dati a persona diversa dal destinatario.

Gli eventi dolosi possono avvenire per comportamenti posti in essere dal personale interno o da soggetti esterni realizzati attraverso:
• distruzione dei documenti;
• accesso non autorizzato;
• furto.

Art. 4

Tipo di violazione

Un incidente sui dati personali può determinare una violazione della:
riservatezza, nel caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
integrità, nel caso di modifica non autorizzata o accidentale dei dati personali;
disponibilità, nel caso di distruzione o perdita accidentale dei dati personali o accesso non autorizzato agli stessi.

Un evento dannoso sui dati personali può integrare anche tutte le tipologie di violazione.

Art. 5

Comunicazione

Chiunque viene a conoscenza di una violazione di sicurezza dei dati personali deve darne comunicazione al Titolare del trattamento, al Responsabile della protezione dati e al Responsabile interno, senza ingiustificato ritardo.

Il personale dipendente e altri collaboratori che prestano le loro attività presso l'Università degli Studi del Sannio, ove dovessero venire a conoscenza di elementi che fanno sospettare (anche a seguito di segnalazione di terzi) che si sia verificato o possa verificarsi un incidente, sono tenuti a comunicare tale circostanza.

L'Autorizzato è tenuto a segnalare con tempestività al proprio responsabile di ufficio e al referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati.

La segnalazione deve essere sempre inoltrata, anche in caso di presunta violazione.
E' compito del Titolare del trattamento, eseguita la valutazione sulla base di quanto emerso dall'analisi dell'evento, stabilire se la violazione riguarda i diritti e le libertà degli interessati.

Art. 6

Doveri

Ogni soggetto sotto la responsabilità del Titolare del trattamento ha l'obbligo di collaborare e seguire le istruzioni che vengono fornite dallo stesso Titolare o da suoi delegati coinvolti nella gestione di una violazione dei dati personali.

E' compito del Responsabile interno o suo Referente assicurare il costante monitoraggio degli adempimenti e delle attività effettuati dai soggetti autorizzati con particolare riferimento alla gestione della comunicazione delle violazioni di dati.

Il Responsabile interno conserva, per quanto di propria competenza, e rende disponibile su richiesta del Titolare o del RPD copia delle comunicazioni delle violazioni di dati personali.

Art. 7

Raccolta delle informazioni

Chiunque viene a conoscenza di una violazione di sicurezza dei dati personali deve raccogliere le informazioni necessarie per consentire al Titolare del trattamento di accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà degli interessati.

Tali informazioni dovranno contenere, se del caso:

- la data di scoperta della violazione;
- 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 di contenimento del danno poste in essere.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Art. 8

Obblighi

Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa può 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 (art. 30 - Regolamento di Ateneo in materia di protezione dei dati personali).