Azienda per il Diritto agli Studi Universitari di TERAMO

DELIBERAZIONE DEL CONSIGLIO DI AMMINISTRAZIONE N. 11 DEL 01/03/2022

OGGETTO: APPROVAZIONE PROCEDURA GESTIONE DATA BREACH

L'anno duemilaventidue, addì uno, del mese di Marzo alle ore 11:00, presso la sede dell'Azienda D.S.U., convocato a termini di regolamento, si è riunito il Consiglio di Amministrazione dell'Azienda, presieduto dal Dott. DI GIACINTO VINCENZO, che, constatata la presenza del numero legale, ha dichiarato validamente costituita la seduta

Interviene l'Arch. SORGI ANTONIO, con funzioni di Segretario.

Prima di dare inizio alla trattazione risultano:

COGNOME E NOME	PRESENTE
DI GIACINTO VINCENZO	SI
PERITO MARIA ANGELA	SI
BENGUARDATO FEDERICA	SI
CIANFAGLIONE COSTANTINO	SI
LANCIONE ALESSANDRO	--

Presenti n° 4 Assenti n° 1

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano,

CONSIDERATO che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- La portata della condivisione e della raccolta di dati personali è aumentata in modo significativa;
- La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

TENUTO PRESENTE che tale evoluzione ha indotto l'Unione Europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dai personali;

DATI ATTO:
che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;
che il GDPR introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate;
che la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- Descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;
- Comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- Descrizione delle probabili conseguenze della violazione dei dati personali;
- Descrizione delle misure adottate o da adottare da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

CONSIDERATO che la violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR;

DATO ATTO che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la

violazione all'interessato senza ingiustificato ritardo, e che tale comunicazione deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali, contenendo obbligatoriamente i seguenti contenuti minimi:

- Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- Una descrizione delle probabili conseguenze dalla violazione;
- Una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi;

CONSIDERATO che l'Azienda ha individuato nella ditta Acta Info sas il soggetto esterno incaricato di svolgere le funzioni previste dal GDPR (RPD) in materia di privacy, visto che l'area delle responsabilità della pubblica amministrazione si è molto ampliata nel tempo e la materia, nella sua specificità, richiede l'apporto di competenze tecniche e di specifica conoscenza della materia, in grado di valutare e studiare le necessità dell'Ente, con la sua peculiare mission e struttura organizzativa;

RILEVATO che, come raccomandato dal suddetto Responsabile esterno per la protezione dei dati (RDP) dell'Azienda, Acta Info sas, è necessario istituire:

1. Una procedura data breach;
2. Un registro interno data breach, dove vendono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere i seguenti dati:

- I dettagli relativi alla violazione (cause, fatti e dati personali interessanti);
- Gli effetti e le conseguenze della violazione;
- I provvedimenti adottati per porvi rimedio;
- Il ragionamento alla base delle decisioni prese in risposta a una violazione;

DATO ATTO:
che la Procedura, avente lo scopo di indicare le modalità di gestione del data breach, garantisce la realizzabilità tecnica e la sostenibilità organizzativa a livello di Ente;
che la Procedura data breach verrà pubblicata sul sito web istituzionale della sezione "Amministrazione Trasparente" sottosezione di secondo livello "Privacy" e ne verrà garantita la conoscibilità della stessa da parte di tutti i dipendenti dell'Ente tramite invio alle mail personali;

ATTESO che gli atti istruttori del presente provvedimento risultano sottoscritti in conformità di quanto previsto dall'art. 8, comma 4, della L.R. n. 91/1994 e che il direttore esprime parere favorevole in ordine alla legittimità e regolarità tecnico amministrativa del provvedimento stesso;

CON VOTI unanimi, legalmente espressi

DELIBERA

Per tutto quanto in premessa, qui da intendere integralmente riportato:

- di approvare la procedura di gestione "DATA BREACH" ai sensi del Regolamento UE n. 679/2016, come da allegato documento che ne costituisce parte integrante e sostanziale;

- di pubblicare il suddetto documento sul sito web istituzionale della sezione "Amministrazione Trasparente" sottosezione "Privacy", garantendo la conoscibilità della procedura tutti i dipendenti dell'Ente tramite invio alle mail personali;

- di trasmettere la presente delibera al Responsabile esterno (RDP) per la protezione dei dati dell'Azienda, Acta Info sas di Addari di Roseto degli Abruzzi (TE);

• di dare atto che il presente provvedimento non comporta impegno di spesa e non è contabilmente rilevante;

dichiarare il presente atto immediatamente eseguibile, ai sensi e per gli effetti dell'art. 13 della L.R. n. 91/1994.

PARERE DI REGOLARITÀ TECNICA

Il Responsabile del Servizio ai sensi del Dlgs 267/2000 e del Regolamento sui controlli interni in ordine alla proposta n.ro 54 del 24/02/2022 esprime parere **FAVOREVOLE.**

Parere firmato digitalmente dal Responsabile del Servizio Dott.ssa DELLA RIPA MARIA CRISTINA in data 24/02/2022

LETTO APPROVATO E SOTTOSCRITTO

Il Presidente	Il Segretario Generale
Dott. DI GIACINTO VINCENZO	l'Arch. SORGI ANTONIO

NOTA DI PUBBLICAZIONE N. 12

Si certifica che copia della presente deliberazione viene pubblicata, ai sensi dell'art. 32 della Legge n. 69 del 18 giugno 2009, all'Albo Pretorio in data 22/03/2022 e che vi rimarrà per 10 giorni consecutivi, ai sensi dell'art. 13 del Regolamento organizzativo dell'Azienda D.S.U. e dell'art. 13 della L.R. 6 dicembre 1994 n. 91.

Teramo, lì 22/03/2022

Il Firmatario della pubblicazione
Dott.ssa DELLA RIPA MARIA CRISTINA

ADSU TERAMO – AZIENDA PER IL DIRITTO AGLI STUDI UNIVERSITARI

PROCEDURA GESTIONE DATA BREACH

1. Che cos'è il Data Breach

Il *data breach* consiste nella violazione dei dati personali gestiti da una organizzazione 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.

Il Regolamento UE sulla protezione dei dati personali, GDPR n. 2016/679, disciplina il *data breach* prevedendo espressamente un obbligo di notifica e comunicazione in capo al titolare del trattamento in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati, quali quelli relativi ai dati sensibili e giudiziari previsti dall'art. 9 del GDPR.

2. Rilevazione identificazione e classificazione degli eventi

La fase di rilevazione, identificazione e classificazione dell'evento è particolarmente critica in quanto comporta o il riconoscimento dell'incidente, e quindi la sua gestione, oppure l'archiviazione dell'evento.

Relativamente alla rilevazione dell'evento, la segnalazione di un evento potenzialmente identificabile come incidente può provenire da diverse fonti, quali:

- personale interno;
- terze parti;
- sistemi di monitoraggio della sicurezza fisica o logica.

Le segnalazioni possono provenire dal servizio di Help Desk, dai sistemisti o dagli utenti stessi. Tutte queste segnalazioni indirizzate vengono analizzate e classificate.

Una volta che l'incidente è identificato e classificato, vengono determinate le seguenti variabili:

- l'urgenza dell'intervento;
- l'impatto dell'evento sull'operatività dell'Amministrazione (es. importanza del servizio impattato);
- nel caso l'evento non presenti conseguenze, esso deve essere comunque tracciato;
- nel caso l'evento venga classificato come incidente di sicurezza deve essere comunicato al Titolare del trattamento, al DPO-RPD Responsabile della protezione dei Dati, al Responsabile del servizio, al CED ove esistente, al fine di avviare la fase di gestione.

3. Gestione degli incidenti

Il processo di gestione degli incidenti è un processo di tipo reattivo. A seguito del verificarsi di un incidente occorre procedere con le attività nel seguito descritte:

- Rilevazione, identificazione e classificazione degli incidenti.
- Gestione degli incidenti.
- Chiusura degli incidenti.

Sulla base delle informazioni raccolte durante la fase di rilevazione, identificazione e classificazione dell'evento, nel caso in cui sia stato classificato come incidente, il Titolare del trattamento o l'IRT se nominato, esegue tutte le procedure necessarie per provvedere alla gestione dello stesso.

Nella gestione di un qualunque incidente di sicurezza devono essere considerate le seguenti due **priorità**:

- Prima Priorità: proteggere tutti gli asset dell'Ente/Azienda, incluse le risorse colpite dall'incidente, fino al ripristino della normale operatività;
- Seconda Priorità: raccogliere informazioni e prove per supportare le eventuali e appropriate azioni correttive, disciplinari o legali.

Ulteriori attività da svolgere collegate all'incidente di sicurezza rilevato:

- nel caso di eventi con livelli di gravità estremamente rilevanti sui dati gestiti dal Sistema informativo l'Ente/Azienda provvederà ad attivare il processo di Data Breach;
- tutte le attività di gestione devono essere tracciate e documentate per quanto possibile a partire dal momento della rilevazione.

4. Processo di Data Breach

Il processo viene attuato nel caso in cui l'incidente di sicurezza abbia un impatto significativo sui dati personali contenuti nelle banche dati (Data Breach) di titolarità dell'Ente, in conformità a quanto previsto dall'art. 33 del GDPR n. 2016/679.

Il flusso inizia con l'identificazione di un Data Breach nell'ambito della gestione di un incidente di sicurezza e si conclude, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, con l'invio al Garante, di una notifica da parte del Titolare del trattamento **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un **apposito registro**. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

5. Descrizione del flusso

Il flusso di comunicazione al Garante da parte dell'Ente prevede i seguenti passi:

1. Il Titolare del trattamento, nel corso della gestione di un incidente di sicurezza informatica, riscontra una compromissione di dati personali (Data Breach).
2. Gli uffici impattati, valutano l'effettiva perdita o diffusione di dati personali e le informazioni contenute nel modulo compilato.
3. In caso di valutazione con rilevamento di violazione dei dati personali, che presenti un probabile rischio per i diritti e le libertà delle persone fisiche, gli uffici impattati informano il Titolare del trattamento inviando le informazioni raccolte.
4. il Titolare del trattamento, di concerto con il DPO/RPPD Responsabile della protezione dei dati, valutano il livello di gravità della violazione in funzione della significatività dell'impatto della violazione avvenuta sui dati personali contenuti nelle banche dati di propria titolarità eseguendo un'autovalutazione attraverso il tool messo a disposizione sul sito web del Garante della protezione dei dati personali accessibile dal seguente link: https://servizi.gpdp.it/databreach/s/self-assessment .

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

Questo strumento, a disposizione di ciascun titolare del trattamento di dati personali, consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il titolare viene guidato nell'assolvimento degli obblighi in materia di **«Notifica di una violazione dei dati personali all'autorità di controllo»** (art. 33Apertura sito esterno in una nuova scheda per l'articolo 33 del Regolamento (UE) 2016/679 del Regolamento (UE) 2016/679 o art. 26 del D.Lgs. 51/2018) e di **«Comunicazione di una violazione dei dati personali all'interessato»** (art. 34Apertura sito esterno in una nuova scheda per l'articolo 34 del Regolamento (UE) 2016/679 del Regolamento (UE) 2016/679 o art. 27 del D.Lgs. 51/2018). Questo strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento dell'Autorità sull'applicazione del Regolamento (UE) 2016/679 o del D.Lgs. 51/2018. Le informazioni fornite durante il suo utilizzo non saranno conservate.

Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 33 del GDPR, la notifica all'autorità di controllo deve essere effettuata entro 72 ore, diminuite a 48 ore per gli Enti della Pubblica Amministrazione secondo quanto previsto dal Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach).

Qualora la notifica all'autorità di controllo sia effettuata oltre i termini previsti, è corredata dei motivi del ritardo.

Eventuali richieste di ulteriori informazioni necessarie o modifiche alla comunicazione al Garante, durante le attività di risoluzione dell'evento, saranno concordate sentito il DPO, Responsabile della Protezione dei Dati, con i responsabili degli uffici coinvolti.

6. Come inviare la notifica al garante

La notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ in attuazione del: Provvedimento del 27 maggio 2021.

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

7. Comunicazione della violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, ai sensi dell'art. 34 del GDPR, comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni:

- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- 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 attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano 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 ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede a una comunicazione pubblica (Es. pubblicazione sul sito web dell'Ente) o a una misura simile, tramite la quale gli interessati sono informati della violazione con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda.

La presente procedura sarà oggetto di periodiche revisioni e adeguamenti in relazione alle norme di armonizzazione che saranno emanate, a variazioni nelle misure di sicurezza da adottare e conseguenti modifiche procedurali.

8. Chiusura degli incidenti

A seguito dell'implementazione delle contromisure e della valutazione della loro efficacia, l'Ente/Azienda dichiara l'incidente chiuso in modo formale, verificando che siano state prodotte le seguenti evidenze:

- l'analisi relativa alle modalità di gestione dell'evento al fine di valutare i tempi di risposta, la metodologia utilizzata, ecc. ed al fine di verificare la necessità di modifiche od integrazioni nella procedura e/o policy in essere;
- la stesura di un rapporto relativo all'incidente di sicurezza, da condividere con i dirigenti responsabili delle strutture coinvolte, in modo da riportare le problematiche di sicurezza verificatesi e tenerne traccia.
  Il rapporto deve essere consegnato tempestivamente e deve contenere, necessariamente, i seguenti punti:
  - descrizione dell'evento, dalla sua segnalazione al ripristino dell'operatività;
  - esposizione di tutte le prove raccolte e di tutte le ricerche effettuate con i relativi risultati;
  - ipotesi sulle cause dell'incidente;
  - proposte di miglioramento e azioni correttive;
  - l'esecuzione delle azioni correttive proposte ed approvate.

Data _____

Il Titolare del trattamento