AZIENDA REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO

Legge Regionale 26 luglio 2002, n. 32 e ss.mm.ii.

DETERMINAZIONE DIRIGENZIALE

N° 568/23 del 12/09/2023

Oggetto: POLICY SULLA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI "DATA BREACH MANAGEMENT": APPROVAZIONE

Servizio proponente: 71.2 PRIVACY GESTIONE ATTI E SUPPORTO RPCT

*Documento informatico firmato digitalmente, ai sensi e con gli effetti del D. Lgs 82/2005 nonché del D.P.R. 445/2000 (e rispettive norme collegate).

IL DIRIGENTE

- Vista la Legge Regionale 26 luglio 2002, n. 32 "*Testo Unico della normativa della Regione Toscana in materia di educazione, istruzione, orientamento, formazione professionale e lavoro*", come modificata dalla Legge Regionale 19 maggio 2008, n. 26 e in particolare l'art.10 della L.R n. 32/2002, come modificato dall'art. 2 della L.R. 26/2008, con cui viene istituita, a far data 1° luglio 2008, l'Azienda Regionale per il diritto allo studio universitario;

- Visto il Decreto del Presidente della Giunta Regionale 8 agosto 2003, n. 47/R recante "*Regolamento di esecuzione della L.R. 26 luglio 2002, n. 32*" e ss.mm.ii.;

- Vista la Delibera della Giunta Regionale Toscana n. 244 del 4 marzo 2019, con la quale si approva il Regolamento organizzativo dell'Azienda;

- Vista la Delibera del Consiglio di Amministrazione dell'Azienda n. 10/19 del 29 marzo 2019 con la quale si prende atto della Delibera di cui sopra, procedendo all'adozione definitiva del Regolamento organizzativo;

- Visto il Provvedimento del Direttore dell'Azienda n. 82/23 del 19 giugno 2023, recante "DETERMINAZIONI IN ORDINE ALL'ADOZIONE DELLA DELIBERAZIONE DEL CDA N. 8/23 DEL 21 FEBBRAIO 2023 RECANTE LA DEFINIZIONE DELLA NUOVA MACRO STRUTTURA ORGANIZZATIVA DELL'AZIENDA REGIONALE DSU TOSCANA: INDIVIDUAZIONE DELLE STRUTTURE ORGANIZZATIVE DI CUI ALL'ART. 16, COMMA 1 LETT. C) DELL'ATTUALE REGOLAMENTO ORGANIZZATIVO (SERVIZIO)" con il quale viene conferito al sottoscritto l'incarico ad interim di Dirigente dell'Area Affari Legali dal 1 luglio 2023 al 30 giugno 2026;

- Visto 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 dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "GDPR");

- Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (di seguito "Codice");

- Considerato che il GDPR detta una complessa disciplina di carattere generale, prevedendo molteplici obblighi e adempimenti in capo ai soggetti che trattano dati personali ed attribuendo, al tempo stesso, al Titolare del trattamento il compito di individuare le modalità operative per porre in essere i prescritti adempimenti;

- Considerato che per "violazione dei dati personali" si intende 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 (art. 4, punto 12), del GDPR e art. 2, comma 1, lett. m), del Decreto;

- Rilevato che, in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare la violazione al Garante 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 presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del GDPR e art. 2-bis del Codice);

- Rilevato, altresì, che il titolare del trattamento è tenuto a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del GDPR anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del Decreto);

- Richiamate le specifiche "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", recanti illustrazione degli obblighi di notifica e comunicazione delle violazioni sanciti dal Regolamento nonché di alcune misure che i Titolari e i Responsabili del trattamento possono intraprendere per soddisfare questi nuovi obblighi, adottate in data 3 ottobre 2017 ed emendate in data 6 febbraio 2018 dal Gruppo di lavoro per la protezione dei dati ex art. 29 (WP29), oggi Comitato Europeo per la Protezione dei Dati (EDPB);

- Richiamate, altresì, le più dettagliate "Linee-guida n. 1/2021" su esempi riguardanti la notifica di una violazione dei dati personali" adottate dallo stesso EDPB in data 14 dicembre 2021;

- Visto i provvedimenti n. 157 del 30 luglio 2019 e n. 209 del 27 maggio 2021 riguardanti la notifica delle violazioni dei dati personali, con i quali il Garante ha indicato le informazioni che i soggetti tenuti alla notifica delle violazioni dei dati forniscono al Garante nell'adempimento dell'obbligo previsto dall'art. 33 del Regolamento e dall'art. 26 del Decreto, nonché le modalità con le quali effettuare la predetta notifica;
- Considerato che in data 05 settembre 2022 è stato designato come Responsabile della Protezione dei Dati (DPO) dell'Azienda, ai sensi dell'art. 37 del Regolamento UE 2016/679, la Società Findata s.r.l.s. con sede legale in Viale Margherita P.co Europa n. 39 Pollena Trocchia (NA) P.I./C.F. 08963651214;
- Valutata la necessità di adottare una procedura interna per la corretta ed efficace gestione delle violazioni dei dati personali (Data Breach) che disciplini puntualmente la prassi da seguire nell'eventualità che si verifichi un evento rischioso;
- Vista la procedura predisposta dal Responsabile del Servizio Privacy, Gestione Atti e supporto RPCT denominata "Policy sulla gestione delle violazioni di dati personali – Data Breach Management –" (allegata alla presente determinazione per farne parte integrante e sostanziale) in cui sono previsti i compiti e le attività da porre in essere entro le 72 ore dal verificarsi dell'evento;
- Visti gli allegati alla procedura che ne costituiscono parte integrante e sostanziale:
    - Allegato A) – Scheda Evento;
    - Allegato B) – Scheda Violazioni Dati;
    - Allegato C) – Registro dei Data Breach;
    - Allegato D) – Modello di comunicazione all'interessato della violazione dei dati personali;
- Dato atto che la procedura di cui sopra, prima della sua redazione finale, è stata condivisa con le seguenti figure aziendali:
    - Amministratore di Sistema aziendale - Ing. Andrea Franci;
    - Responsabile Servizio Sistemi Informatici e Applicativi (ICT) - Dott.ssa Sonia Chiantini;
    - Responsabile Servizio Protocollo - Dott. Marco Aleksy Commisso;
    - Referente Servizio Privacy aziendale - Dott. Mirko Carli;

che costituiscono il gruppo di intervento di primo livello per gli incidenti sulla privacy aziendale (Privacy Incident Group);

- Dato atto, altresì, che la procedura, così come redatta nei contenuti, è stata validata dal Responsabile della Protezione dei dati Personali (DPO) aziendale;

DETERMINA

1. Di approvare la procedura aziendale "Policy sulla gestione delle violazioni di dati personali – Data Breach Management –" (allegata alla presente determinazione per farne parte integrante e sostanziale) che contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016;
2. Di dare mandato al Servizio Privacy, Gestione Atti e Supporto RPCT affinché provveda alla pubblicazione della procedura nella sezione "Privacy" e "Amministrazione Trasparente" del sito aziendale;
3. Di dare, altresì, mandato al Servizio Privacy, Gestione Atti e Supporto RPCT di garantire la massima diffusione e conoscibilità della procedura agli organi e dipendenti aziendali;
4. Di assicurare la pubblicità integrale dell'atto mediante pubblicazione all'Albo online dell'Azienda.

Il Dirigente ad interim
Area Affari Legali
Dott. Enrico Carpitelli
(Firmato digitalmente)*

*Documento informatico firmato digitalmente, ai sensi e con gli effetti del D. Lgs 82/2005 nonché del D.P.R. 445/2000 (e rispettive norme collegate).