

**AZIENDA TERRITORIALE PER L'EDILIZIA RESIDENZIALE
MATERA**

L'anno duemilaventitre il giorno venti del mese di novembre, l'Amministratore Unico dell'Azienda, Avv. Lucrezia Guida, nominato con decreto del Presidente del Consiglio Regionale n. 9 del 20 ottobre 2019, assistita dal Direttore F.F. Ing. Pasquale Lionetti, con funzioni anche di Segretario, ha adottato la seguente:

DELIBERAZIONE N. 0111/2023 DEL 22/11/2023

Oggetto: Approvazione Piano di protezione dei dati personali e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016

FORMULAZIONE DI PARERI:

Il Responsabile del Procedimento, dott. Michele Salvatore Bianco _____

Il Direttore F.F. Ing. Pasquale Lionetti: parere di regolarità tecnica favorevole _____

Il Direttore F.F. Ing. Pasquale Lionetti: parere di legittimità favorevole _____

L'AMMINISTRATORE UNICO

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è 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 significativo;
- 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 CONTO 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 dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

DATO ATTO che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

RILEVATO che, con il GDPR, è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

RICHIAMATA la Legge 25 ottobre 2017, n. 163 e, in particolare, l'art. 13, che ha delegato il Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

RILEVATO che il decreto legislativo delegato è finalizzato a realizzare l'adeguamento della normativa nazionale al GDPR sulla base dei seguenti *principi e criteri direttivi* specifici:

- a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
- b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
- c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;
- d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;
- e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse;

RITENUTO che l'adeguamento dell'ordinamento nazionale interno al GDPR renda necessario definire le politiche e gli obiettivi strategici da conseguire per garantire l'adeguamento;

DATO ATTO che, sulla base del delineato quadro normativo, l'obiettivo di fondo del GDPR è la sicurezza del trattamento dei dati personali, programmando e pianificando gli interventi affinché i dati personali siano:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatto salvo l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

RITENUTO che l'obiettivo di assicurare la sicurezza dei dati richiede di gestire efficacemente, e conformemente alle disposizioni del GDPR, il rischio di violazione dei dati derivante dal trattamento, per tale dovendosi intendere 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 e che, a tal fine, vadano definiti gli obiettivi correlati alla gestione del rischio;

CONSIDERATO che la norma UNI ISO 31.000 contiene le indicazioni sulla predisposizione e attuazione dei *Piani di trattamento del rischio* e, sulla base del *principio di tracciabilità documentale*, le opzioni di trattamento individuate e attuate;

Ritenuto, pertanto, necessario procedere alla approvazione di un piano di protezione dei dati personali e di gestione del rischio di violazione;

Visto l'allegato schema di Piano ed i relativi Allegati di seguito elencati:

- 01 - STRUTTURA ORGANIZZATIVA ED ELENCO SOGGETTI INTERNI ED ESTERNI
- 02 - SCHEDE DI RICOGNIZIONE TRATTAMENTI ED INDICE MAPPA TRATTAMENTI
- 03 - SCHEDE DI VALUTAZIONE DI IMPATTO DPIA TRATTAMENTI A RISCHIO ELEVATO
- 04 - SCHEDE DI SINTESI DPIA
- 05 - MAPPE DEI LUOGHI
- 06 - MAPPE HARDWARE SOFTWARE ARCHIVI E BANCHE DATI ELETTRONICHE
- 07 - MISURE DI PROTEZIONE DATI
- 08 - MAPPA EVENTI RISCHIOSI E MOTIVAZIONI DI STIMA
- 09 - MODELLI ATTI DI DELEGA ED INCARICO AL TRATTAMENTO DATI
- 10 - PROGRAMMAZIONE CORSI DI FORMAZIONE

Appurato che:

- lo schema di piano copre il periodo del triennio 2023-2025
- la funzione principale dello stesso è quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di

sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale;

- il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre più incisivi;
- l'adozione del documento non si configura come un'attività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione;
- eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD;

Considerato che lo schema di Piano è stato predisposto dal responsabile del procedimento con il coinvolgimento e la partecipazione degli attori indicati nello Schema di Piano medesimo;

RILEVATO il Responsabile del procedimento è il dott. Michele Salvatore Bianco Funzionario dell'Unità Operativa Sistema Informativo Aziendale e Transizione Digitale;

DATO ATTO che, al fine di garantire il livello essenziale delle prestazioni, il presente provvedimento deve essere lo schema di piano allegato devono essere pubblicati sul sito web dell'Amministrazione, nella apposita sezione "Amministrazione trasparente" e nella sottosezione "Altri contenuti-anticorruzione";

Visti:

- Legge n. 241/1990;
- D.Lgs. n. 196/2003;
- Legge n. 190/2012;
- D.Lgs. n. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto dell'Ente;
- Regolamento di organizzazione degli uffici e dei servizi;
- Codice di comportamento interno dell'Ente;

Visto il parere favorevole espresso dall'Ing. Pasquale Lionetti, in qualità di Direttore F.F. in ordine alla regolarità tecnica e alla legittimità del presente atto;

DELIBERA

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. di approvare l'allegato schema di Piano di protezione dei dati personali e di gestione del rischio di violazione, nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n.679/2016 i cui Allegati, numerati da 01 a 10, sono depositati in atti presso il competente Ufficio;
2. di dare atto che il Piano recepisce le politiche e gli obiettivi strategici dell'ente e costituisce, unitamente alle altre misure adottate dal titolare, lo strumento per l'attuazione di dette politiche e obiettivi;
3. di dare atto che il Piano copre il periodo di un triennio, 2023-2025 ed è soggetto ad aggiornamento annuale, e ad aggiornamenti anche infrannuali correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi ovvero alla necessità di conformarsi a provvedimenti e/o pareri dell'autorità di controllo o del RPD;
4. di comunicare i contenuti del Piano a tutti i soggetti indicati nel Piano medesimo, attraverso i canali dallo stesso individuati, e di demandare ai Dirigenti nonché a tutti i dipendenti l'attuazione del Piano;
5. di disporre che al presente provvedimento venga assicurata la pubblicità legale e la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali" e il regolare flusso delle informazioni e dei dati dal Responsabile del procedimento (flusso in partenza) al Responsabile della trasparenza (flusso in arrivo), in modo tale che la pubblicazione venga assicurata nei tempi e con modalità idonee ad assicurare l'assolvimento dei vigenti obblighi di pubblicazione;
6. di dare atto che, in disparte le pubblicazioni sopra indicate, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.Lgs. n. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.Lgs. n. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.
7. di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.Lgs. n. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.
8. di dichiarare la presente deliberazione immediatamente esecutiva.

IL DIRETTORE F.F.
(Ing. Pasquale Lionetti)

L'AMMINISTRATORE UNICO
(Avv. Lucrezia Guida)

La presente Deliberazione n° 0111/2023 del 22/11/2023 è stata pubblicata nell'Albo Pretorio on-line del sito web di Matera (www.atermaterita.it) dal 22/11/2023 per rimanere pubblicata per giorni 15 (quindici).

Matera, li 22/11/2023

IL FUNZIONARIO RESPONSABILE DEGLI AFFARI GENERALI
(dott.ssa Annalisa Chiara Giordano)