

Consorzio per lo Sviluppo Industriale  
della Provincia di Potenza

## DELIBERA

N° 92 del 6 Giugno 2019

**OGGETTO:** Adozione del “Regolamento per la Protezione dei dati personali e particolari ai sensi e in attuazione del Regolamento UE 2016/679”

### IL COMMISSARIO STRAORDINARIO

*del Consorzio per lo Sviluppo Industriale della Provincia di Potenza*

**VISTA** la L.R. n.18 del 5 febbraio 2010, pubblicata sul B.U.R. n.7 del 5 febbraio 2010, recante “*Misure finalizzate al riassetto e al risanamento dei Consorzi per lo sviluppo industriale*”;

**VISTA** la L.R. n.32 del 5/11/2014, pubblicata su B.U.R. n.43 del 7/11/2014 recante “*Risanamento e rilancio dei Consorzi per lo sviluppo industriale*” con cui, tra l’altro, sono state introdotte modifiche ed integrazioni alla predetta L.R. n.18/2010;

**VISTA** la L.R. n. 34 del 30.11.2017 “*Disposizioni in materia di Consorzi per lo Sviluppo Industriale*”, pubblicata sul BUR Basilicata n. 47 del 30.11.2017;

**VISTO** lo Statuto del Consorzio per lo Sviluppo Industriale della Provincia di Potenza approvato ai sensi della L.R. n.5 novembre 2014 n.32 e pubblicato sul B.U.R. Regione Basilicata n.20 dell’1/06/2016;

**VISTA** la delibera di Giunta Regionale n.1009 del 2.10.2018 con la quale il Dott. Aniello ERTICO è stato nominato Commissario Straordinario del Consorzio per lo Sviluppo Industriale della Provincia di Potenza;

**VISTA** la delibera n.1 dell’8.10.2018 avente ad oggetto L.R. n. 34 del 30.11.2017 recante “*Disposizioni in materia di Consorzi per lo Sviluppo Industriale*”, art.1: “*Art. 21 della L.R. 18/2017 – Disposizioni transitorie e urgenti*”. Nomina Commissario Straordinario del Consorzio per lo Sviluppo Industriale della Provincia di Potenza – Insediamento, con la quale si è formalmente insediato il Commissario Straordinario Dott. Aniello ERTICO;

**VISTA** la delibera n. 2 dell’11 ottobre 2018 avente ad oggetto “*Art. 7 L.R. n. 32 del 5.11.2014 – Conferma Direttore del Consorzio per lo Sviluppo Industriale della Provincia di Potenza*”;

**VISTA** la delibera di Giunta Regionale n. 250 del 4.04.2019 avente ad oggetto “*Art.1 comma 2 Legge Regionale 30.11.2017, n. 34 – DGR n. 109/2018. Differimento scadenza durata in carica del Commissario Straordinario del Consorzio per lo Sviluppo Industriale della Provincia di Potenza*”;

**PREMESSO** che il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR- *General Data Protection Regulation*) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

**CHE** il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, che prevede:

**Articolo 30 - Registri delle attività di trattamento**

- 1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
  - a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
  - b) le finalità del trattamento;
  - c) una descrizione delle categorie di interessati e delle categorie di dati personali;
  - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
  - e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
  - f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
- 2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
  - a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
  - b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
  - c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
  - d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
- 3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
- 4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
- 5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia

occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

### **Articolo 35 Valutazione d'impatto sulla protezione dei dati**

- 1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
- 2. Il titolare del trattamento, allorché svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
- 3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
  - a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
  - b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
  - c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
- 4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
- 5. L'autorità di controllo [...]
- 7. La valutazione contiene almeno:
  - a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
  - b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
  - c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
  - d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
- 8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
- 9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
- 10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplina il trattamento

*specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.*

- 11. *Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.*

**CHE** il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (di seguito "Regolamento"), ha stabilito, all'art. 9, par. 1, un generale divieto di trattamento dei dati sensibili, oggi denominati "categorie particolari di dati personali", cioè dei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

**CHE** L'art. 9, par. 2, lett. g, del Regolamento sancisce tuttavia una deroga a tale divieto, rispetto al trattamento delle richiamate categorie di dati necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Analoghe considerazioni possono in parte essere formulate in relazione ai dati relativi a condanne penali e reati di cui all'art. 10 del Regolamento.

**CHE** il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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 è stato modificato con il D.Lgs. 10 agosto 2018, n. 101

**CHE**, nelle more dell'approvazione delle prime linee guida che il Garante per la privacy emanerà a seguito di quanto previsto all'art. 154-bis del Codice della privacy come da ultimo modificato dal già menzionato D.Lgs. 101/2018, si rende tuttavia necessario procedere con l'attività prevista dalle norme espressamente citate;

**CHE** Il legislatore nazionale ha definito "rilevante" l'interesse pubblico per il trattamento effettuato da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie indicate dal comma 2 dell'art. 2-sexies, del d.lgs. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali (di seguito "Codice", come recentemente modificato dal d.lgs. n. 101/2018).

**CHE** più in particolare, nella medesima disposizione viene altresì specificato che i trattamenti in questione sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, «nei casi previsti dalla legge», di regolamento. Tali fonti normative devono specificare i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (cfr. art. 2-sexies, comma 1 per le particolari categorie di dati personali,

nonché art. 2-octies, commi 3 e 5, per i dati relativi a condanne penali e reati e a connesse misure di sicurezza).

**CHE** la Nota dell'Autorità Garante al Presidente del Consiglio dei Ministri, al Presidente della Conferenza delle regioni e delle province autonome e al Presidente dell'ANCI, in tema di trattamenti di categorie particolari di dati personali per motivi di interesse pubblico rilevante del 5/12/18 consiglia l'adozione/adequamento dei regolamenti comunali sulla protezione dei dati personali e particolari.

**RILEVATO:** Che vanno adottate misure di sicurezza adeguate che riducano al minimo il rischio di violazione/perdita di dati e/o di informazioni e/o illecite diffusioni o comunicazioni a terzi.

**CHE** tutto ciò che si presenta come un rischio per la sicurezza lo è anche per la privacy e, quindi, è necessario preventivamente valutare i rischi (mediante audit ed elaborazione di DPIA) e così prevenire eventuali perdite di dati.

**CHE** il titolare deve identificare i flussi di dati personali relativi a ogni trattamento e mantenerli aggiornati in un inventario dei trattamenti di dati personali, in linea con quanto prescritto dall'art.30 del Regolamento.

**CHE** il titolare o responsabile deve identificare, definire e documentare le basi legali per il trattamento dei dati personali individuati.

**CHE** il titolare deve individuare e attuare le misure di sicurezza dei dati personali relative alla protezione dei dati personali e mantenere attive e aggiornate quelle già adottate in precedenza anche seguendo quanto emerso dall'ambito della "Protezione dei dati personali *by design* e *by default*".

**CHE** il titolare deve stabilire un processo documentato di gestione degli incidenti relativi alla protezione dei dati personali, in ambito ICT, che includa:

- la valutazione e la gestione delle violazioni dei dati personali e procedure per mitigare il danno causato da tali violazioni;
- le modalità di notifica alle autorità di controllo (entro 72 ore dalla presa di conoscenza della violazione), nel caso l'organizzazione sia titolare del trattamento, di ogni violazione dei dati personali che potrebbe causare un rischio per i diritti e la libertà delle persone fisiche;

**CHE** il titolare deve stabilire un processo per un semplice e tempestivo accesso ai diritti degli interessati.

**CHE** il paragrafo 1 dell'art. 32 del Regolamento richiede che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e la libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio". Questo richiede che venga svolta l'analisi dei rischi che insistono sui sistemi utilizzati per il trattamento dei dati, al fine di garantire riservatezza, integrità e disponibilità.

**CHE** l'identificazione dei rischi e la conseguente mappatura è preliminare all'analisi dei rischi del trattamento di dati personali e andrebbe effettuata su più livelli (art. 35 GDPR).

Che si deve tenere conto dello stato dell'arte e dei costi di adeguamento, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

**CHE** nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

**CHE** il titolare del trattamento fa sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

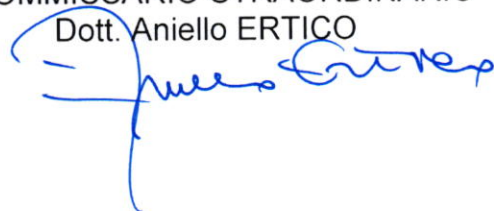
**RITENUTO** pertanto opportuno procedere alla sua approvazione per permettere a questa Amministrazione di provvedere con immediatezza all'attuazione del Regolamento UE 2016/679;

Tutto quanto sopra premesso e considerato, con i poteri conferitigli con Delibera di Giunta Regionale n. 1009 del 2 ottobre 2018;

## **DELIBERA**

1. di approvare il Regolamento attuativo del Regolamento UE 2016/679 in materia di protezione dati personali e particolari, che consta di n. 36 articoli e allegati n. 8 che viene allegato al presente atto per costituirne parte integrante e sostanziale attuativo del Codice in materia di protezione dei dati personali di cui al D.Lgs. 30 giugno 2003, n. 196.
2. di trasmettere formalmente copia del regolamento al Responsabile per la Protezione Dati.

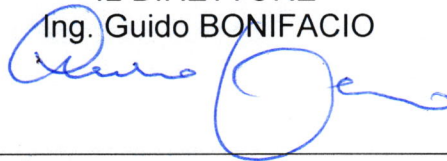
IL COMMISSARIO STRAORDINARIO  
Dott. Aniello ERTICO



**Visto del Direttore:**

Si attesta la legittimità dell'atto.

IL DIRETTORE  
Ing. Guido BONIFACIO



Tito li, 05/062019