REGOLAMENTO PRIVACY ARPAC MULTISERVIZI S.R.L.

INDICE

INTRODUZIONE

Il 27 aprile 2016 il Parlamento Europeo ha approvato il Regolamento Europeo (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati di tutti i cittadini in Europa eliminando le differenze di approccio tra Stati membri. Il nuovo regolamento ha trovato applicazione, in tutte le Pubbliche Amministrazioni e aziende private che trattano i dati personali, in tutti gli stati membri a decorrere dal 25 maggio 2018.

Il Regolamento UE n.679/2016 (di seguito GDPR) ha come oggetto la tutela delle persone con riguardo alla circolazione dei dati, il suo principio cardine è la tutela del diritto e delle libertà fondamentali alla protezione dei dati (ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano- art 8 par.1 Carta dei diritti fondamentali dell' Unione Europea e art. 16 par.1 del trattato sul funzionamento dell' Unione Europea) nonché il principio generale alla portabilità e circolazione dei dati personali nell'UE (art.1,2,3 GDPR). Per rafforzare la protezione, il GDPR introduce numerose e rilevanti novità partendo da un approccio fondato sul principio di cautela ponendo l'accento sulla responsabilizzazione (accountability) dei titolari (come la valutazione d'impatto, le misure di sicurezza e la nomina di un DPO). La nuova disciplina europea pone con forza l'accento sulla "accountability, ossia sulla responsabilizzazione dei Titolari e sull'adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Una delle misure necessarie da adottare è il *data protection by default and by design,*ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Il GDPR ha obbligato le amministrazioni pubbliche e private ad adeguarsi alle nuove regole in modo tale da assicurare un livello elevato di protezione dei dati che riguardano le persone fisiche, equivalente in tutti gli Stati membri, così da rimuovere gli ostacoli alla circolazione dei dati personali all' interno dell' Unione Europea.

In questo contesto il presente regolamento in materia di privacy rappresenta uno strumento utile per ottenere maggiore equilibrio tra i contrapposti interessi dei soggetti coinvolti, come ad esempio il rapporto tra i dipendenti dell'ARPAC Multiservizi e gli enti e/o le società o persone fisiche che sono in contatto con la società.

Al fine di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, l'ARPAC Multiservizi S.r.l. ha avviato un processo di aggiornamento e revisione delle attività connesse alla protezione dei dati personali, al fine di consentire un innalzamento dell' attuale livello di protezione di questi ultimi.

L'ARPAC Multiservizi S.r.l. ha adottato il presente regolamento al fine di dotarsi di un modello di " governance" e di presidi organizzativi in linea con le nuove previsioni del Regolamento europeo 2016/679 (GDPR).

QUADRO NORMATIVO DI RIFERIMENTO

- **REGOLAMENTO 2016/679** codice in materia di dati personali relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
- **D.LGS. 101/2018** di adeguamento della normativa interna al GDPR.
- **Legge 25 ottobre n. 163** recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **Norme internazionali** sulla circolazione dei dati personali;
- **Regolamento Arpac per il controllo analogo degl organismi partecipati,** deliberazione n. 304 del 20/0572019;
- **MOGC 231,** Decreto legislativo n. 231 del 2001;
- **Piano triennale della prevenzione della corruzione dell' Arpac multi servizi S.r.l.,** approvato con delibera n. 22 del 7/4/2022.

DEFINIZIONI

Normativa Privacy: Complessivamente, il Regolamento europeo (UE) 2016/679 del Parlamento Europeo, e del Consiglio, la normativa italiana di riferimento(in particolare il D.Lgs come modificato e integrato dal D.Lgs 101/2018 di adeguamento , nonché le regole di condotta /regole tecniche ed esso allegate e i Provvedimenti dell'Autorità Garante per la protezione dei dati personali).
GDPR: Il Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
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 mediante uno o più elementi identificativi quali il nome, il numero di telefono un identificativo online etc., ovvero mediante uno o più elementi caratteristici della sua identità fisica, genetica, culturale economica o sociale;
Interessato: la persona fisica cui si riferiscono i dati personali;
Titolare del trattamento: la persona fisica o giuridica che determina le finalità del trattamento, le modalità e i mezzi del trattamento;
DPO: Soggetto designato dal titolare del trattamento in funzione delle sue qualità professionali al fine di informare e fornire consulenza al Titolare stesso nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa privacy;
Persone autorizzate al trattamento: le persone fisiche autorizzate da Arpac Multiservizi S.r.l. a compiere operazioni di trattamento dei dati personali, nell' ambito e sotto l' autorità dell'Arpac Multiservizi S.r.l. in ottemperanza alle istruzioni ricevute.
Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che non sia l'interessato, il Titolare del trattamento, il DPO e le persone autorizzate al trattamento dei dati personali sotto l' Autorità diretta del Titolare.
Trattamento: qualsiasi operazione compiuta con o senza l' ausilio di processi automatizzati e applicata ai dati personali come la raccolta, la registrazione, la strutturazione, la conservazione l'adattamento,la modifica, l'uso, l'estrazione, la consultazione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Tuttavia le autorità pubbliche che possono ricevere comunicazioni di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
Limitazione del trattamento: il contrassegno dei dati personali conservati con l' obiettivo di limitarne il trattamento in futuro;
Principio di minimizzazione: adottare misure minime e tecniche organizzative in grado da assicurare che i dati vengano trattati per le finalità del trattamento;
Pseudonomizzazione: il trattamento del dato personale in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l' utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

Profilazione: qualsiasi forma di trattamento automatizzato dei dati personali consistente nell'utilizzo di dati personali per valutare determinati aspetti relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, il comportamento, l' affidabilità, l'ubicazione o gli spostamenti di detta persona fisica.
Consenso dell' interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell' interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Dati appartenenti a particolari categorie: i dati personali idonei a rilevare l' origine razziale o etnica , le convinzioni religiose, le opinioni politiche, l' adesione a partiti, sindacati, associazioni, dati relativi alla salute, alla vita sessuale o all' orientamento sessuale della persona;
Dati giudiziari: I dati personali relativi a condanne penali e reati ai sensi dell'art.10 del GDPR, nonché i dati idonei a rilevare i provvedimenti di cui all'art. 3 comma 1 lettere *a,r,u* del D.P.R. 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe o delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di procedura penale.
Dati genetici: i dati personali relativi alle caratteristiche ereditarie o genetiche di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica.
Dati relativi alla salute: i dati personali attinenti ala salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rilevano informazioni relative al suo stato di salute;
Diffusione: la trasmissione di dati personali a soggetti indeterminati in qualunque forma;
Rischio:possibilità che un evento non voluto e potenzialmente dannoso si verifichi facendo venir meno la riservatezza e/integrità e/o disponibilità dei dati personali , e quindi mettendo a repentaglio la tutela dei diritti e le libertà delle persone fisiche;
Danno: conseguenza pregiudizievole derivante dal concretizzarsi di una minaccia.
Data breach: Violazione della sicurezza che comporta, accidentalmente o volontariamente la distruzione, perdita, alterazione, pubblicazione o accesso non autorizzato di dati personali trasmessi, conservati o in altro modo trattati.
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
Banca dati: Una banca dati è una raccolta di informazioni/dati, in forma cartacea o informatica, organizzati in modo strutturato e omogeneo, in modo da poter essere facilmente reperite, aggiornate e modificate attraverso l'utilizzo di apposite chiavi di ricerca.
Cancellazione sicura: Eliminazione di dati presenti sul supporto elettronico e/o cartaceo con le modalità che li rendano inintelligibili e non recuperabili.

ART. 1 OGGETTO

Il presente regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche e dei dipendenti dell'ARPAC Multiservizi S.r.l., in ordine al trattamento dei dati personali effettuato dal Titolare del trattamento, nel rispetto di quanto previsto dal GDPR.

ART. 2 OBIETTIVI DEL PRESENTE DOCUMENTO

Il presente Regolamento definisce la portata e l'attuazione della normativa *Privacy*all' interno dell'ARPAC Multiservizi S.r.l., in particolare delinea un sistema organico e strutturato di gestione di tutti gli aspetti concernenti i profili "*privacy*" attraverso un modello di gestione uniforme, fornendo ai soggetti che di tale sistema fanno parte indicazioni chiare sia sul piano tecnico/operativo che sul piano organizzativo, sulle modalità di applicazione della normativa *Privacy.* Il presente documento pertanto definisce i requisiti per il trattamento dei dati personali affinchè esso avvenga all'interno del quadro delineato dalla Normativa *Privacy,* nel rispetto delle prescrizioni previste dalla normativa stessa e individua gli adempimenti da porre in essere per garantire la conformità alla normativa. Il Titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi sono gestiti conformemente alle disposizioni del GDPR, del D.LGS. 101/2018 e del presente Regolamento.

ART. 3 PRINCIPI E LICEITA'

Nel presente Regolamento vengono integralmente recepiti i principi del GDPR per effetto dei quali i dati personali sono trattati:

- in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime e successivamente trattati con modalità compatibili con le suddette finalità;
- esatti e se necessario aggiornati e pertanto vengono adottate tutte le misure necessarie per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- in maniera da garantire un' adeguata sicurezza dei dati personali compresa la protezione mediante misure tecniche e organizzative adeguate;

In ordine alla liceità:

- il trattamento è lecito solo se l'interessato ha espresso il consenso al trattamento dei dati personali;
- il trattamento è lecito solo se necessario all' esecuzione di un contratto di cui l'interessato è parte o all' esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo legale al quale è soggetto il Titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell' interessato;

- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

ART. 4 CONDIZIONI PER IL CONSENSO

Ai fini del trattamento dei dati personali ilconsenso deve essere esplicito, libero, autonomo,specifico e informato e il titolare deve essere sempre in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento. Il consenso dell'interessato è prestato con dichiarazione scritta attraverso la compilazione di un modulo predisposto dal titolare previa consegna e presa d'atto dell'informativa sulla privacy. La richiesta del consenso deve essere presentata in forma comprensibile utilizzando un linguaggio chiaro e semplice. L'interessato ha diritto di revocare il proprio consenso in qualsiasi momento e la revoca non pregiudica la liceità del trattamento basata sul consenso liberamente prestato.

ART. 5 INFORMATIVA

Il Titolare al momento della raccolta dei dati personali è tenuto a fornire all'interessato un' apposita informativa redatta per iscritto secondo le modalità previste dal GDPR, e dal presente regolamento, redatta in forma concisa, chiara, trasparente e utilizzando un linguaggio semplice. L'informativa è fornita mediante appositi moduli da consegnare agli interessati e contiene obbligatoriamente i seguenti dati:

- identità e dati di contatto del titolare;
- identità e dati di contatto del DPO;
- finalità del trattamento;
- i destinatari dei dati personali;
- la base giuridica del trattamento;
- se il titolare trasferisce i dati personali a Paesi Terzi;
- il periodo di conservazione;
- il diritto dell' interessato di chiedere la rettifica o la cancellazione;
- il diritto di presentare reclamo all' autorità di controllo.

Nel fornire l'informativa il titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base al quale è effettuato il trattamento dei dati sensibili e giudiziari.

ART. 6 RUOLI E RESPONSABILITA'

➢ INTERESSATO

Con il termine interessato si fa riferimento alla persona fisica resa identificata o identificabile mediante i dati personali trattati (a titolo esemplificativo ma non esaustivo: dipendenti, committenti, collaboratori esterni ecc).

➢ TITOLARE DEL TRATTAMENTO

Il "Titolare è la persona fisica/giuridica che determina le finalità e i mezzi del trattamento dei Dati Personali disciplinando le attività che comportano il trattamento dei dati personali. Il "Titolare" ha facoltà di nominare persone autorizzate al trattamento impartendo a queste ultime specifiche istruzioni riguardo al trattamento dei dati personali e allo svolgimento di operazioni che riguardano i dati personali.

➢ DPO/RDP

Il Titolare designa il Responsabile della protezione dei dati (DPO/RDP). Il DPO, opera alle dipendenze del Titolare che mette a sua disposizione le risorse necessarie per adempiere ai suoi compiti e accedere al trattamento dei dati personali. E' tenuto al segreto e alla riservatezza in merito all' adempimento dei propri compiti, deve essere in possesso di un adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, deve adempiere le sue funzioni in totale indipendenza e in assenza di conflitto di interesse.
Il DPO svolge i seguenti compiti:

- informa e fornisce consulenze al Titolare del trattamento nonché ai dipendenti che eseguono trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento;
- fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati personali;
- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all' esercizio dei diritti;
- funge da punto di contatto con il Garante della privacy per la protezione dei dati personali per questioni connesse al trattamento dei dati tra cui la consultazione preventiva.

➢ *PERSONE AUTORIZZATE AL TRATTAMENTO*

Le" Persone autorizzate al trattamento" sono soggetti all'uopo autorizzati dal Titolare nell'ambito dei rispettivi ruoli. Ciascuna Persona Autorizzata al trattamento opera sulla base delle istruzioni fornitegli. Le suddette istruzioni possono essere differenziate e sono aggiornate nel corso della durata del rapporto o in ragione di specifiche necessità (cambio mansione/responsabilità e/o attività). Le Persone autorizzate eseguono le proprie attività lavorative nel rispetto delle normative applicabili e delle istruzioni ricevute dal Titolare del trattamento in merito alla corretta modalità di gestione dei dati personali. Trattano i dati personali garantendo l'adozione delle misure di sicurezza disposte dal Titolare al fine di evitarne la distruzione e/o la perdita o l'accesso di persone non autorizzate. E' tenuto a verificare costantemente la correttezza dei dati trattati e, ove necessario provvedere al loro aggiornamento, garantendo in ogni operazione la massima riservatezza,astenendosi dal comunicare o diffondere a terzi, salvo previa autorizzazione del Titolare. Deve adottare tutte le misure per evitare l'accesso a terzi in caso di allontanamento dalla propria postazione di lavoro e segnalare eventuali criticità inerenti la gestione della privacy. Infine è tenuto a partecipare alle iniziative formative su tematiche privacy.

➢ *AMMINISTRATORE DI SISTEMA*

L'Amministratore di Sistema, individuato nell' Ufficio del Supporto Informatico, sovrintende alla gestione e alla manutenzione delle banche dati e al sistema informatico di cui è dotata l'ARPAC Multiservizi S.r.l..
L'Amministratore di sistema svolge attività quali:

- monitora lo stato dei sistemi di elaborazione e delle banche dati dell'Arpac Multiservizi con particolare costante attenzione al profilo della sicurezza;
- verifica che l'accesso ai sistemi e ai dati personali ivi contenuti sia debitamente protetto, nonché consentito solo nel rispetto della legge;
- il salvataggio dei dati, l' organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware;
- opera una valutazione del rischio informatico;
- adotta i sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici;
- effettua gli interventi di manutenzione necessari;
- verifica il corretto funzionamento del *backup/recovery;*
- avvisa tempestivamente il Titolare del Trattamento riguardo ad eventuali violazioni della sicurezza da cui possa derivare la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l' accesso non autorizzato ai dati personali trattati dall' Arpac Multiservizi S.r.l.;
- presta la massima collaborazione nei confronti del Titolare del Trattamento e del DPO.

ART.7 MISURE DI SICUREZZA

Il Titolare del trattamento dei dati personali garantisce l'applicazione di adeguate misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta. In particolare il Titolare del trattamento mette in atto misure tecniche, organizzative, di gestione, procedurali e documentali idonee allo scopo di garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono:

- lapseudonomizzazione e la cifratura dei dati personali;
- procedure per assicurare in modo permanente la riservatezza, l' integrità e la disponibilità dei sistemi e dei servizi di trattamento;
- modalità per garantire il ripristino tempestivo dell' accesso ai dati personali in caso di incidente tecnico e fisico;
- un procedura per testare, verificare e valutare regolarmente l' efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

ART.8 LA VALUTAZIONE D'IMPATTO

La valutazione d' impatto (**D.P.I.A.**)è un processo volto a descrivere il trattamento, valutarne la necessità e proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento. E' un onere posto direttamente a carico del Titolare del Trattamento previsto dall' art.35 GDPR.. Con tale valutazione si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, il livello d'impatto va calcolato sugli interessati non sul titolare. Preliminarmente alla DPIA deve essere effettuata o aggiornata ala ricognizione dei trattamenti e deve essere effettuata la determinazione in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati. La **D.P.I.A.** deve essere **di procedere al trattamento dei dati personali**nel caso in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Se il Titolare dovesse ritenere sussistenti i rischi per le libertà e i diritti degli interessati, dovrà individuare le misure specifiche richieste per

attenuare o eliminare tali rischi. Solo nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di Controllo (consultazione preventiva).

La **D.P.I A**. deve contenere almeno:

- la descrizione sistematica dei trattamenti previsti, le finalità del trattamento, compreso la base giuridica utilizzata dal Titolare;
- la valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;
- la valutazione dei rischi per i diritti degli interessati;
- le misure previste per affrontare i rischi, inclusi le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone.

La **D.P.I.A**. implica l'analisi e la descrizione delle aree critiche da esaminare, del profilo di tutti i soggetti coinvolti, gli effetti e le conseguenze del trattamento dei dati e una valutazione dei rischi collegati. Il titolare deve inoltre consultarsi con il DPO quando svolge una valutazione d' impatto, il DPO a sua volta deve fornire il parere e sorvegliarne lo svolgimento.

Quando insorgono variazioni del rischi, rappresentati dalle attività relative al trattamento, il Titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati. Per conseguire l' obiettivo della riduzione del rischio la DPIA, si svolge attraverso le fasi previste dall' art. 35 paragrafo 7 del GDPR ovvero:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso l' interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1 dell' art. 35 del GDPR;
- le misure previste per affrontare 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.

I Titolare del Trattamento, nello svolgere l' attività di valutazione, si consulta con il DPO , e laddove emerga la presenza di rischi elevati, il Titolare, su impulso del DPO, è tenuto a richiedere la consultazione preventiva dell' autorità di controllo in relazione al trattamento ai sensi dell' art. 36 del GDPR.

ART. 9 ORGANIZZAZIONE INTERNA ALL' ARPAC MULTISERVIZI IN MATERIA DI PRIVACY

- **Titolare del trattamento dei dati**: il Titolare del Trattamento dei dati è l'ARPAC Multiservizi (P.IVA 04709971214) con sede a Napoli alla via Nuova Poggioreale n. 11 ed. 5, rappresentata dall' A.U. pro tempore;
- **Incaricati/autorizzati**: i responsabili delle aree dell'ARPAC Multiservizi e i dipendenti a cui sono state affidate mansioni che comportano il trattamento dei dati personali;
- **DPO:** nominato con delibera dell' A.U.;
- **Amministratore di sistema:** individuato nell' ufficio di supporto informatico;

L'ARPAC Multiservizi S.r.l., in persona dell' **A.U.,Titolare del Trattamento**è responsabile:

- di assicurare che le misure di sicurezza e procedurali adottate e le modalità operativo/gestionali siano conformi ai requisiti definiti dalla normativa privacy anche attraverso l'effettiva ed efficace attuazione delle linee guida contenute nel presente regolamento.
- di assicurare costantemente che i compiti e le responsabilità in materia di protezione dei dati personali siano allocati in modo chiaro e appropriato, in modo coerente con le mansioni lavorative assegnate.
- di organizzare, gestire, e supervisionare tutte le operazioni di trattamento dei dati personali effettuate dai dipendenti dell'ARPAC Multiservizi S.r.l., in modo che il trattamento dei dati personali avvenga sempre nel rispetto dei principi previsti dall'art. 5 del GDPR (liceità, correttezza, trasparenza, esattezza, integrità, limitazione delle finalità riservatezza e minimizzazione);
- di valutare, di concerto con il DPO, i rischi correlati alle attività di trattamento dei dati personali, tenuto conto delle modalità operative dell'ARPAC Multiservizi S.r.l., dell'organizzazione interna e delle misure di sicurezza;
- di assicurare la presenza delle misure tecniche e organizzative monitorandone costantemente la corretta applicazione di concerto con il supporto informatico e il DPO;
- di gestire le attività necessarie per consentire l'esercizio dei diritti da parte degli interessati al fine di fornire riscontro alle loro istanze;
- di gestire il processo di *data breach*, provvedendo all'alimentazione e conservazione dell'apposito registro e all'eventuale notifica della violazione al Garante dei dati personali, di concerto con il DPO.

➢ **Persone autorizzate al trattamento:** L' ARPAC Multiservizi ha provveduto ad autorizzare al trattamento i dipendenti che, nell' ambito delle mansioni attribuite, siano a contatto con i dati personali nei termini riportati dal presente regolamento. I soggetti in parola sono autorizzati al trattamento dei dati personali per le sole finalità indicate dall'ARPAC Multiservizi ed espressamente precisate ed elencate nel presente regolamento nel rispetto del GDPR. E' vietato qualsiasi altro utilizzo dei dati personali che non sia in linea con l' incarico ricevuto. Il personale autorizzato, infatti, è stato formalmente edotto che il trattamento e la conservazione deve avvenire in modo lecito e nel rispetto della riservatezza, che la raccolta e la registrazione dei dati, mediante strumento elettronico o cartaceo, deve essere corretta e aggiornata qualora l' interessato o il Titolare ne facciano richiesta e deve essere limitata alle necessità dell' ARPAC Multiservizi.

➢ **DPO:** L'ARPAC Multiservizi ha provveduto a nominare un DPO (Responsabile della Protezione dei Dati) che ha la funzione di affiancare il Titolare, l'Amministratore di sistema e le Persone Autorizzate al trattamento affinchè sia assicurata una corretta gestione dei dati seguendo i principi e le indicazioni inserite nella normativa vigente – GDPR- e nel presente Regolamento. Nominato con delibera n. 13 dell' A.u.pubblicata il 16/03/2021, è raggiungibile ai seguenti indirizzi :

➢ Email DPO: privacy@arpacmultiservizi.it

➢ Email :segr.generale@arpacmultiservizi.it

➢ **Amministratore di sistema**L'Amministratore di sistema svolge attività quali:

➢ monitora lo stato dei sistemi di elaborazione e delle banche dati dell' Arpac Multiservizi S.r.l. con particolare costante attenzione al profilo della sicurezza;

- verifica che l'accesso ai sistemi e ai dati personali ivi contenuti sia debitamente protetto, nonché consentito solo nel rispetto della legge;
- il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware;
- opera una valutazione del rischio informatico;
- adotta i sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici;
- effettua gli interventi di manutenzione necessari;
- verifica il corretto funzionamento del *backup/recovery;*
- provvede all'aggiornamento semestrale delle password;
- avvisa tempestivamente il Titolare del Trattamento e il DPO riguardo ad eventuali violazioni della sicurezza da cui possa derivare la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l' accesso non autorizzato ai dati personali trattati dall'ARPAC Multiservizi S.r.l.
- presta la massima collaborazione nei confronti del Titolare del Trattamento e del DPO.

ART.10 GESTIONE DEI DATI PERSONALI

L'ARPAC Multiservizi S.r.l. garantisce che i dati raccolti siano completi, accurati e mantenuti aggiornati rispetto al proposito per cui vengono raccolti, compatibilmente con le tempistiche necessarie e tenuto conto del numero dei dati oggetto di trattamento. I dati personali sono raccolti solo ed esclusivamente per le finalità specifiche ed esplicite indicate nell'informativa privacy.
Gli interessati hanno facoltà di esercitare i seguenti diritti in merito ai propri dati personali:

- **diritto di accesso** (art.15): ovvero il diritto di ottenere la conferma che sia o meno in corso il trattamento dei dati che lo riguardano e in tal caso di ottenere l'accesso ai dati personali, ottenendone copia;
- **diritto di rettifica**(art.16): ovvero il diritto di ottenere la rettifica dei dati inesatti che lo riguardano o l'integrazione dei dati incompleti;
- **diritto alla cancellazione(diritto all'oblio)**(art.17): ovvero il diritto di ottenere la cancellazione dei dati che lo riguardano, se sussiste uno dei motivi indicati nell' art 17 GDPR:
  1) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
  2) l' interessato revoca il consenso su cui si basa il trattamento conformemente all' art 6, par 1, lett. a, o all' art. 9 par. 2 lett. a, e se non sussiste altro fondamento giuridico per il trattamento;
  3) l'interessato si oppone al trattamento ai sensi dell'art. 21 par.1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell' art. 21 par. 2(finalità di marketing diretto);
  4) i dati personali sono trattati illecitamente;
  5) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato cui è soggetto il Titolare del trattamento;
  6) i dati personali sono stati raccolti relativamente all' offerta di servizi della società di informazione di cui all' art.8 par.1.(condizioni applicabili al consenso dei minori);

- **diritto alla limitazione del trattamento** (art.18): ovvero il diritto di ottenere, nei casi indicati dall' art. 18 GDPR, la cancellazione/pseudonomizzazione/anonimizzazione dei dati personali che lo riguardano con l' obiettivo di limitarne il trattamento;
- **diritto alla portabilità dei dati** (art.20): ovvero il diritto, nei casi indicati dall' art.20 GDPR (ossia il trattamento effettuato con mezzi automatizzati, basato sul consenso o sull' esecuzione di un contratto), di ricevere, in formato strutturato e leggibile da dispositivo automatico i dati che lo riguardano, compresa la profilazione sulla base personale, nonché di trasmettere tali dati ad un altro Titolare del trattamento senza impedimenti;
- **diritto di opposizione** (art.21): ovvero il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano;

In caso d'esercizio da parte dell' interessato di uno dei diritti elencati, il Titolare provvede a dare seguito alla richiesta.

ART. 11 FASI DEL CICLO DI VITA DEL DATO

Le operazioni di trattamento del dato devono essere strettamente limitate a perseguire le finalità indicate nell' informativa privacy cosi come pubblicata sul sito dell' ARPAC Multiservizi S.r.l. esse consistono nella raccolta, nel trattamento e cessazione con conseguente cancellazione;

raccolta: per quanto concerne la raccolta dei dati, l'acquisizione può avvenire sia in forma cartacea che attraverso i canali digitali(posta elettronica). Il trattamento dei dati Personali da parte dell' ARPAC Multiservizi S.r.l. deve avvenire per il perseguimento di finalità legittime individuate anticipatamente e comunicate agli interessati che devono essere informati utilizzando un linguaggio semplice e chiaro.

trattamento: il titolare tratta i dati con le modalità previste nel GDPR, nel D.Lgs 101/2018 e nel presente Regolamento, effettuando periodicamente l' aggiornamento e la ricognizione dei dati.

cessazione del trattamento e cancellazione: Nel caso in cui l'ARPAC Multiservizi S.r.l. decida di cessare lo svolgimento di una o più operazioni di trattamento, i dati personali utilizzati nel contesto di tali operazioni devono essere distrutti, salvo gli adempimenti legati ad obblighi di legge. L'ARPAC Multiservizi S.r.l. provvede alla distruzione dei documenti e alla cancellazione dai supporti informatici che, dopo essere stati utilizzati per il trattamento,siano destinati ad altro scopo (es. assegnazione di un pc ad altro dipendente)in ottemperanza a quanto disposto dalla normativa.

ART.12 MISURE ORGANIZZATIVE

Misure valide per tutto il personale:

L'ARPAC Multiservizi S.r.l. ha identificato il personale addetto a ciascun trattamento limitando l'attività di trattamento al solo personale identificato che ha ricevuto istruzioni operative nel rispetto dei seguenti principi:

- trattamento dei dati esclusivamente per le finalità e le modalità individuate dall' ARPAC Multiservizi S.r.l., nel rispetto delle leggi vigenti;

- limitazione del trattamento dei dati alle seguenti attività: raccolta,registrazione, organizzazione, elaborazione, archiviazione, consultazione, estrazione, utilizzo, comunicazione e cancellazione;
- trattamento limitato ai dati strettamente necessari in relazione alle finalità individuate;
- rispetto delle misure di sicurezza per la conservazione/archiviazione della documentazione cartacea, in particolare l' obbligo di chiusura a chiave degli armadi e la rimozione delle chiavi prima della chiusura quotidiana degli uffici;
- divieto di comunicazione a terzi delle password e credenziali di accesso personali;
- divieto di comunicazione/trasmissione di dati a terzi in assenza do documentazione cartacea e in assenza di un a causa giustificativa prevista dalla legge;
- divieto di divulgazione dei dati personali;
- utilizzo di dispositivi elettronici(anche mobili) assegnati esclusivamente dall'Arpac Multiservizi S.r.l. per finalità lavorative e nel rispetto delle istruzioni ricevute.

ART.13 MISURE TECNICHE

Misure di sistema

L'accesso ai sistemi informatici è concesso solo all' Amministratore di Sistema ed ai dipendenti nominati . Il sistema prevede l'accesso ai sistemi informatici tramiti l' utilizzo di identificativi univoci per ciascun utente attraverso l' adozione di password di complessità adeguata(lunghezza minima di 8 caratteri, contenenti lettere maiuscole e minuscole, numeri e caratteri speciali) che va aggiornata a cadenza semestrale.

Misure di sicurezza dei personal computer

- Attivazione del blocco automatico dei PC dopo un determinato intervallo temporale di utilizzo;
- installazione dei software firewall e antivirus sui PC, installazione periodica di aggiornamenti di sicurezza del sistema operativo sui PC;
- effettuazione periodica di backup per i dati eventualmente presenti sul PC e disabilitazione della modifica delle impostazioni di sicurezza dei PC degli utenti.

Sicurezza di smartphone e tablet

Accesso alle funzionalità e applicazioni tramite PIN o password, selezione/impostazione di blocchi per l' accesso ai dati e/o alla condivisione tramite applicazioni gestite da soggetti terzi, con riferimento alla rubriche sulle e-mail, connessione mobile da internet sicura(sim card dedicata protetta da password).

Sicurezza di rete

- Adozione di impostazioni di sicurezza adeguate per la connessione tramite LAN e limitare la possibilità di installazione di software e di download da parte degli operatori;
- adozione di impostazioni di sicurezza adeguate per le connessioni WI-FI, quali l'utilizzo di protocolli di criptazione aggiornati;
- accesso alla rete da remoto locale sicuro; installazione periodica degli aggiornamenti per la sicurezza dei sistemi.

Sicurezza dei dati

- Effettuazione semestrale di copie backup dei dati memorizzati su sistemi informatici centralizzati o sui singoli PC e verifica della loro integrità;

- adozione di adeguate misure di sicurezza fisica per il sito presso il quale sono custodite le copie di backup(es. controllo accessi fisici ai locali, misure antincendio);
- cancellazione sicura o distruzione dei dati su supporto informatico o cartaceo quando il loro trattamento non è più necessario o in occasione di dismissione di dispositivi informatici(PC, smartphone, hard-disk);
- utilizzo di e-mail che garantisca adeguati livelli di sicurezza e adozione di antivirus e antispam per le caselle e-mail.

Sicurezza fisica

- Protezione degli uffici con sistema di sicurezza di chiusura porte in grado di impedire l'accesso, se non mediante forzatura, a soggetti estranei non muniti di chiave;
- custodia dei documenti cartacei e dei dispositivi di memorizzazione contenenti dati personali in spazi chiusi(es. archivi,armadi), in locali con accesso consentiti solo ai dipendenti autorizzati;
- identificazione e manutenzione delle fonti calore nei locali dove sono custoditi i documenti cartacei(si intende anche le sole tubature elettriche idrauliche e gas).

ART. 14 CONTRATTI CON TERZE PARTI

L'ARPAC Multiservizi S.r.l. si relaziona con il Socio Unico(l'Agenzia Regionale per l' Ambiente della Regione Campania) e con atri soggetti (consulenti e collaboratori esterni) con i quali condivide dati, informazioni e risorse. Tutto ciò espone l' ARPACMultiservizi S.r.l. a numerosi rischi derivanti dall' acceso e utilizzo, da parte di terzi, di "dati personali", pertanto viene richiesto a tali soggetti il rispetto delle regole contemplate nel presente regolamento, nel GDPR e nella normativa sulla privacy. Il Titolare del Trattamento, di concerto con il DPO, definisce gli obblighi cui devono attenersi le terze parti, a tal fine vengono individuati i livelli di sicurezza in funzione delle informazione condivise e i requisiti di sicurezza opportuni per tutelare le informazione condivise con le "terze parti".

ART. 15 DATA BREACH

Si definisce "*Data breach*" una "violazione dei dati personali", ovvero ogni evento che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'acceso ai dati personali a persone non autorizzate. Si elencano di seguito tre categorie di violazioni:
Violazione di riservatezza: divulgazione o accesso a dati personali non autorizzato o accidentale;
Violazione di integrità: alterazione dei dati personali non autorizzata o accidentale;
Violazione di disponibilità: perdita, inaccessibilità o distruzione, accidentale o non autorizzata, di dati personali.
In caso di data breach i dipendenti dell'ARPAC Multiservizi S.r.l. sono tenuti ad avvisare immediatamente il DPO, il quale avvierà le opportune consultazioni con l'Autorità Garante.
La comunicazione all'Autorità Garante deve contenere:

- la responsabilità degli autori coinvolti;

- le finalità e i mezzi del trattamento previsto;
- i risultati della valutazione d'impatto effettuata;
- ogni altra informazione eventualmente richiesta dall' Autorità Garante.

L'Autorità Garante, in via preventiva, può richiedere informazioni relative a segnalazioni degli interessati coinvolti, può raccogliere documentazione relativa alle misure tecniche e organizzative adottate. Tali richieste devono essere prodotte in breve termine. Nel caso di violazione dei dati personali, l'ARPAC Multiservizi S.r.l. deve notificare l'evento all' Autorità Garante entro 72 ore dal momento in cui lo stesso viene rilevato.
A titolo esemplificativo, ma non esaustivo, gli eventi possibili di violazione possono essere costituiti da :

- **Distruzione dei dati informatici o documenti cartacei**: intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi, conseguente ad eliminazione logica (ed es .errata cancellazione dei dati nel corso di interventi di ripristino) o fisica (es. rottura dei dispositivi di memorizzazione informatica, incendio/allagamento dei locali dove sono archiviati i documenti).
- **Perdita di dati**: conseguente a smarrimento/furto di supporti informatici o di altri documenti cartacei;
- **Accesso non autorizzato o intrusione a sistemo informatici**, tramite lo sfruttamento di vulnerabilità dei sistemi interni o delle reti di comunicazione;
- **Modifica non autorizzata dei dati**, derivante ad es. da un'erronea esecuzione di interventi suoi sistemi di informatici;
- **Rivelazione di dati e documenti a soggetti terzi non legittimati,** anche non identificati, autorizzati, conseguenti ed es. alla fornitura di informazioni, anche verbali, a soggetti diversi dal personale dipendente autorizzato.

ART. 16 COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI

Nel caso in cui la violazione esponga l'Interessato a particolari rischi, verrà effettuata una notificazione, senza ritardo, della violazione stessa all'Interessato. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura e l'entità della violazione del dato.
Non è richiesta la comunicazione all'interessato se il Titolare del trattamento ha messo in atto tutte le misure tecniche e organizzative adeguate, e già adottate in precedenza, come ad esempio l' utilizzo di strumenti di crittografia o cifratura tali da rendere il dato inaccessibile e incomprensibile . La comunicazione non è altresì richiesta qualora il titolare abbia adottato successivamente le misure atte a scongiurare il sopraggiungere del rischio elevato per i diritti e le libertà degli interessati.
Nel caso in cui il Titolare non provveda a comunicare in tempo, all'interessato, la violazione dei dati personali, l'autorità di controllo può richiedere che vi provveda, previa valutazione sull'entità della violazione.

ART. 17 SANZIONI

L'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell' Autorità di controllo ai sensi dell'art.58 par.2 del GDPR, o il negato accesso in violazione dell'art. 58 par 1 del GDPR, comporta sanzioni pecuniarie.

Inoltre, la violazione della normativa privacy può avere impatti reputazionali negativi anche rilevanti sull' ARPAC Multiservizi S.r.l.. Pertanto, il Titolare, avvalendosi dell'ausilio del DPO, attua periodicamente controlli sul processo di gestione degli adempimenti Privacy, con l'obiettivo di rilevare lo stato di conformità rispetto alla normativa Privacy, nonché alle disposizioni contenute nel presente documento.
L'accertamento di determinate violazioni può anche comportare l' emissione , da parte del Titolare,su impulso del DPO,di ordini di cancellazione dei Dati Personali raccolti o l'interruzione di determinate operazioni di Trattamento che si assumono illecite.
Infine gli Interessati possono promuovere azioni di risarcimento per i danni subiti a causa dello svolgimento di operazioni di Trattamento riguardanti i loro Dati personali che non siano conformi alla Normativa Privacy.

ART.18 DISPOSIZIONI FINALI

Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice, del GDPR, nonché le Linee Guida e i provvedimenti del Garante.

Il presente Regolamento recepisce e si adegua alla normativa vigente in materia di riservatezza e protezione dei dati personali.