COMUNE DI ARVIER

Modello Organizzativo Privacy – MOP

(Regolamento UE 2016/679)

Approvato con Deliberazione di Giunta Comunale n. 40 del 17.04.2026

INDICE

1. Premessa

Il presente Modello Organizzativo Privacy (MOP) è redatto ai sensi del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 come novellato dal D.Lgs. 101/2018, nonché delle disposizioni settoriali applicabili alla Pubblica Amministrazione (tra cui D.Lgs. 33/2013 in materia di trasparenza, D.Lgs. 82/2005 – Codice dell'Amministrazione Digitale (CAD), D.Lgs. 36/2023 in tema di appalti pubblici e Legge 241/1990 sul procedimento amministrativo).

Scopo del MOP è descrivere in maniera organica le misure organizzative, procedurali e tecniche messe in atto dall'Ente Pubblico per assicurare un trattamento dei dati personali conforme ai principi di liceità, correttezza e trasparenza, nonché al principio di accountability previsto dall'art. 5, par. 2, GDPR.

Attraverso l'adozione del presente documento l'Ente intende:

- individuare ruoli e responsabilità interne in ambito privacy;
- definire istruzioni operative per autorizzati e designati;
- garantire la tenuta del registro dei trattamenti e la gestione dei rischi;
- documentare le misure di sicurezza applicate;
- descrivere il processo di gestione di data breach e di risposta ai diritti degli interessati.

Il presente documento deve essere oggetto di aggiornamento periodico, al fine di garantire la sua costante adeguatezza rispetto alle modifiche dell'assetto organizzativo e strutturale dell'Ente; all'evoluzione normativa in materia di protezione dei dati personali; a variazioni nei trattamenti svolti o nei rischi rilevati.

L'aggiornamento è di competenza del Titolare del trattamento, anche su proposta del Responsabile della Protezione dei Dati (DPO), e deve essere tracciato e documentato.

2. Il Titolare del trattamento

Ai sensi dell'art. 4 n. 7 GDPR è titolare del trattamento il **Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), C.F. 80003210079 / P.IVA 00140870072, protocollo@pec.comune.arvier.ao.it** in quanto autorità pubblica che determina finalità e mezzi dei trattamenti effettuati nell'esercizio dei propri compiti istituzionali e di pubblico interesse (art. 6, par. 1, lett. e GDPR).

2.1. Missione istituzionale dell'Ente

In accordo con quanto dichiarato all'art 3 dello Statuto,

1. Il Comune promuove lo sviluppo ed il progresso civile, sociale ed economico della propria comunità, su base autonomistica, ispirandosi ai principi, valori ed obiettivi della costituzione, delle leggi statali, delle leggi regionali e delle tradizioni locali.

2. Il Comune persegue la collaborazione e la cooperazione con tutti i soggetti pubblici e privati, promuovendo la piena partecipazione dei cittadini e delle forze sociali, economiche e sindacali all'amministrazione della comunità.

3. La sfera di governo del Comune è costituita dal proprio territorio di competenza.

4. Il Comune persegue con la propria azione i seguenti fini:

a. il superamento degli squilibri economici, sociali e territoriali esistenti nel proprio ambito nonché il pieno sviluppo della persona umana, alla luce dell'uguaglianza e della pari dignità sociale dei cittadini;

b. la promozione della funzione sociale dell'iniziativa economica pubblica e privata, anche mediante lo sviluppo dell'associazionismo economico o cooperativo;

c. il sostegno alla realizzazione di un sistema globale ed integrato di sicurezza sociale e di tutela della persona, in sintonia con l'attività delle organizzazioni di volontariato;

d. la tutela e lo sviluppo delle risorse naturali, ambientali, storiche e culturali presenti sul proprio territorio per garantire alla comunità locale una migliore qualità di vita;

e. la tutela e lo sviluppo delle consorterie e dei consorzi di Miglioramento Fondiario, nonché la protezione ed il razionale impiego dei terreni consortili, dei demani collettivi e degli usi civici nell'interesse delle

comunità locali, con il consenso di queste ultime, promuovendo a tal fine l'adeguamento degli statuti e dei regolamenti delle consorterie alle esigenze delle comunità titolari;

f. la salvaguardia dell'ambiente e la valorizzazione del territorio come elemento fondamentale della propria attività amministrativa;

g. la valorizzazione ed il recupero delle tradizioni e consuetudini locali, anche in collaborazione con i comuni vicini e con la regione; h. la piena attuazione della partecipazione diretta dei cittadini alle scelte politiche ed amministrative degli enti locali, della regione e dello stato.

5. Il Comune partecipa alle associazioni nazionali, regionali ed internazionali degli enti locali, nell'ambito dell'integrazione europea ed extra-europea, per la valorizzazione del ruolo essenziale dei poteri locali ed autonomi.

Poiché dettati da atti normativi vigenti nel diritto nazionale, tali funzioni costituiscono la base giuridica primaria dei trattamenti di dati personali eseguiti (art. 6, par. 3 GDPR; art. 2-ter D.Lgs. 196/2003).

2.2 Organigramma dell'Ente

Figura professionale	Cat.	Pos.	Orario	Posti Dotazione Organica	Ricoperti	Vacanti	Note
Servizio Amministrazione Generale e di Segreteria							
Aiuto collaboratore (Op. amm.)	C	C1	36/36	1	1	0	Demografici, Elettorale e Protocollo *Part-time concesso anche per l'anno 2026*
Collaboratore (Istr. amm.)	C	C2	36/36	1	1	0	Segreteria
Aiuto bibliotecario	C	C2	36/36	1	1	0	Bibliotecaria
Servizio Finanziario							
Funzionario (Istr. Dir. Finanziario)	D	D	36/36	1	1	0	
Edilizia pubblica - Tecnico manutentiva Acquisizione di beni e servizi							
Collaboratore (Geometra)	C	C2	36/36	2	2	0	
Funzionario (Specialista informatico)	D	D	36/36	1	1	0	*Part-time concesso per l'anno 2026*
Capo operatore (Cantoniere-autista)	B	B3	34,5/36	1	1	0	Part-time al 95,83%
Operatore (Cantoniere-autista)	B	B2	36/36	1	1	0	
Edilizia privata							
Funzionario (Istr. Dir. Tecnico)	D	D	36/36	1	1	0	Responsabile Servizio Associato Part-time concesso per l'anno 2026
Polizia Locale							
Aiuto collaboratore (Vigile-messo-autista)	C	C1	36/36	1	1	0	
Aiuto collaboratore (Vigile-messo)	C	C1	36/36	1	1	0	
Posti Vacanti							
Collaboratore (Istr. Amm.)	C	C2	36/36	1		1	Cessato il 30/9/2024
TOTALI				**13**	**12**	**1**	

Al Comune di Arvier sono assegnati n. 2 Segretari per l'esercizio associato dell'Ambito n. 3 ai sensi della L.R. 6/2014:

Figura professionale	Posti	Ricoperti	Vacanti	Note
Segretario	2	2		Responsabili Servizio Amm. generale, Segreteria (personale), Biblioteca e PL

3. Autorizzati al trattamento e designati al trattamento

Conformemente all'art. 29 GDPR e all'art. 2-quaterdecies del Codice Privacy, il Titolare designa, con atto formale, il personale che tratta dati

personali sotto la sua autorità. In questa definizione sono inclusi i dipendenti, collaboratori, membri di commissioni che trattano i dati personali di proprietà del Titolare del trattamento, sotto dirette istruzioni scritte impartite sulle procedure da seguire.

Ogni designato/autorizzato:

- riceve idonea formazione periodica (cfr. Sez. XVI);
- sottoscrive impegno di riservatezza;
- opera nei limiti del principio di minimizzazione.

3.1. L'atto di nomina

L'atto di nomina ad autorizzato al trattamento deve essere predisposto su carta intestata del Titolare del trattamento e sottoscritto sia dal legale rappresentante del Titolare sia dal soggetto autorizzato. Tale atto ha la finalità di formalizzare l'autorizzazione ai dipendenti ad accedere alle banche dati e alle informazioni del Titolare esclusivamente in relazione alle mansioni effettivamente svolte. L'accesso ai dati avviene secondo il principio di necessità e di minimizzazione, per cui ciascun soggetto è autorizzato a trattare solo specifiche categorie di dati, strettamente funzionali al raggiungimento delle finalità connesse al proprio ruolo. Ne consegue che non tutti i dipendenti possono accedere indistintamente a tutti i dati del Titolare, ma solo a quelli pertinenti e indispensabili allo svolgimento delle attività assegnate. L'atto di nomina rappresenta quindi uno strumento essenziale per garantire un trattamento dei dati conforme alla normativa vigente e per assicurare una chiara attribuzione di responsabilità all'interno dell'organizzazione.

Atto di nomina a soggetto autorizzato al trattamento

Il Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), nella sua qualità di Titolare del trattamento dei dati, ai sensi del combinato disposto degli artt. 29 del Reg. UE 2016/679 e 2quaterdiecies D.Lgs. 196/2003, così come novellato dal D.Lgs. 101/2018,

Designa

il Sig./la Sig.ra ..... (C.F.: .....), in servizio presso ..... con la mansione di ..... quale autorizzato al trattamento.

In quanto soggetto autorizzato del trattamento, Ella avrà accesso a tutti i dati contenuti nelle seguenti banche dati e/o archivi:

1. archivi cartacei relativi ai fascicoli degli utenti del Titolare, fascicoli relativi alle pratiche professionali e personali dei singoli professionisti dell'Ente e degli eventuali collaboratori interni ed esterni;
2. archivi informatici sul personal computer della postazione;
3. account di posta elettronica dell'Ente;
4. archivi informatici sul server e/o cloud dell'Ente

e, comunque, ad ogni altra informazione necessaria per lo svolgimento delle mansioni affidate.

Le finalità per le quale Ella viene autorizzata al trattamento dei dati personali sono le seguenti:

- .....
- .....

Con riferimento alle banche dati e/o archivi a cui ha accesso, Ella dovrà compiere le seguenti operazioni (privilegi di accesso):

1. consultare i documenti presenti sia negli archivi cartacei che in quelli informatici presenti della sede di lavoro, estrarne copia, elaborare dati ivi contenuti, comunicarne il relativo contenuto agli interessati, ove richiesto in tal senso dal Titolare e previa espressa autorizzazione del Titolare medesimo e dopo aver accertato l'identità del richiedente;
2. adottare, durante le operazioni di trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare del trattamento e, in particolare, dovrà:
   a) quando appositamente autorizzato all'accesso alle banche dati informatiche, custodire con attenzione le proprie credenziali di autenticazione ed ogni dispositivo che le contiene, ed evitare di operare su terminali altrui e/o di lasciare accessibile il sistema operativo in caso di allontanamento, anche temporaneo, dal posto di lavoro, al fine di evitare trattamenti non autorizzati;
   b) trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
   c) conservare i supporti informatici e/o cartacei contenenti i dati personali, in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
   d) con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
   e) copie di dati personali oggetto di trattamento devono essere effettuate esclusivamente se necessario e soltanto previa autorizzazione del titolare del trattamento;

f) in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al titolare del trattamento;
g) segnalare al titolare del trattamento eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine 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 alle finalità della raccolta;
h) effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal titolare del trattamento e secondo le modalità stabilite dai medesimi per la loro identificazione;
i) mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
l) svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal titolare del trattamento e, comunque, in modo lecito e secondo correttezza;
m) fornire al titolare del trattamento, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;

3. Per l'esecuzione della mansione, verranno trattati i seguenti dati:

.....

4. l'autorizzato si impegna a osservare quanto indicato nella presente nomina;
5. nel caso di inadempimento agli obblighi sanciti dalla presente, l'Autorizzato potrà essere oggetto di procedimenti disciplinari ai sensi di legge e del CCNL applicato.

Data .....

Firma del titolare del trattamento
Comune di Arvier

.....

Per presa visione
Firma autorizzato del trattamento

.....

Registro degli autorizzati al trattamento

Nome e cognome	Data di nomina	Mansione

4. Responsabili del trattamento esterni – art. 28 GDPR

L'art. 4 par. 8 Reg. UE 679/2016 definisce il responsabile del trattamento:

***Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.*

In altri termini, laddove l'Ente affidi attività a terzi (p. es. servizi IT, conservazione digitale, postalizzazione massiva), tali soggetti sono nominati **Responsabili del trattamento** tramite contratto/atto di nomina che contempla: oggetto, durata, categorie di dati, misure di sicurezza, sub-fornitura. L'atto, redatto per iscritto, deve essere sottoscritto dai legali rappresentanti del Titolare e del Responsabile.

4.1 Check-list per la qualifica dei Responsabili esterni

Per la scelta dei Responsabili del trattamento viene utilizzata una checklist di valutazione dei fornitori, finalizzata a verificare che gli stessi presentino requisiti adeguati di affidabilità, competenza ed esperienza in materia di protezione dei dati personali. La checklist è fornita già in fase di gara o di affidamento e costituisce uno strumento di supporto alla verifica delle misure tecniche e organizzative adottate dal fornitore in conformità al GDPR.

Nel caso in cui alla procedura partecipino più fornitori, il bando di gara deve prevedere l'obbligo, per ciascun concorrente, di produrre un'autocertificazione attestante l'esperienza maturata e le competenze possedute in materia di sicurezza dei dati personali; tale dichiarazione ha valore esclusivamente informativo e non comporta l'attribuzione di punteggi. In fase di affidamento, la checklist viene trasmessa al fornitore individuato, che è tenuto a compilarla in ogni sua parte e a sottoscriverla per il tramite del legale rappresentante, con successivo invio via PEC al Titolare del trattamento.

La checklist viene quindi analizzata con il supporto del DPO, al fine di valutare se il fornitore sia in grado di garantire un livello di sicurezza adeguato rispetto ai trattamenti che verranno svolti. In caso di esito positivo, si procede con l'affidamento dell'incarico e con la formale nomina a Responsabile del trattamento. In caso di esito negativo, l'affidamento non può essere disposto e si procede alla selezione di un diverso fornitore, in coerenza con le Linee guida EDPB n. 7/2020, secondo cui il Responsabile esterno deve essere scelto dal Titolare sulla base di garanzie adeguate in termini di sicurezza e protezione dei dati personali

Schema di Check list

ai sensi dell'art.28 del Reg. UE 2016/679

A1) Anagrafica Responsabile del trattamento	
A2) Oggetto del trattamento	descrivere dettagliatamente il servizio esplicitando le <u>finalità</u> del trattamento di dati personali
A3) Tipologia di dati personali trattati	□ comuni/identificativi □ semi sensibili (patrimoniali/economici) □ particolari (salute, religiosi..., biometrici) □ dati giudiziari

1- Generale

1.1	E' garantito il ripristino dei dati anche a seguito di incidente tecnico?	□ Si entro _____ ore	□ No

1.2	Nelle peggiori ipotesi è garantita la continuità operativa?	□ Si con garanzia di perdita massima di lavoro per le ultime _____ ore	□ No
1.3	Se applicabile, è previsto l'utilizzo di un server secondario per emergenze a garanzia della continuità operativa?	□ Si	□ No
1.4	E' stato nominato un Responsabile della protezione dei dati personali? (RPD/DPO)	□ Si	□ No
1.5	Sono state individuate le persone autorizzate alla gestione dei dati personali per il trattamento oggetto di nomina?	□ Si	□ No
1.6	Il soggetti autorizzati al trattamento hanno ricevuto istruzioni su come trattare i dati personali?	□ Si	□ No
1.7	Sono organizzate sessioni formative per i soggetti autorizzati al trattamento?	□ Si ogni ___ mesi	□ No
1.8	E' stato predisposto e mantenuto aggiornato il registro dei trattamenti per il trattamento in oggetto di affidamento?	□ Si ogni ___ mesi	□ No
1.9	Il trattamento prevede il trasferimento dei dati ad altri soggetti (persone giuridiche)?	□ Si Nome organizzazione:_____ Per le finalità di: _____	□ No
1.10	Il trattamento prevede trasferimenti di dati a soggetti con sede fuori UE?	□ Si Nome organizzazione:_____ Per le finalità di: _____	□ No
1.11	L'Azienda ha conseguito certificazioni di qualità?	□ Si _____	□ No
1.12	Il trattamento è effettuato con Vs. server o server di terze parti in modalità cloud (saas, iaas, paas), raggiungibili da browser? □ Si □ No	Si utilizzano server qualificati Ag.Id ? □ Si □ No	
1.13	Se il trattamento (A2) prevede l'utilizzo di saas, il software è qualificato Ag.Id?	□ Si □ No	

2- Backup

2.1	Sono mantenute copie di dati all'interno dell'organizzazione?	□ Si □ Si, con crittografia ogni ___ ore indirizzo di conservazione _____	□ No
2.2	Sono mantenute copie di dati all'esterno dell'organizzazione? (disaster recovery)	□ Si □ Si, con crittografia ogni ___ ore indirizzo di conservazione _____ □ Cloud AgId nome fornitore _____	□ No
2.3	Sono mantenute copie di dati conservate offline (su memorie di massa isolate dalla rete)	□ Si □ Si, con crittografia ogni ___ ore indirizzo di conservazione _____	□ No

3- Restore

3.1	E' garantito il ripristino dei dati anche a seguito di incidente tecnico?	□ Si entro _____ ore	□ No
3.2	E' garantita la continuità operativa?	□ Si con garanzia di perdita massima di lavoro per le ultime _____ ore	□ No
3.3	Se applicabile, è previsto l'utilizzo di un server secondario per emergenze a garanzia della continuità operativa?	□ Si	□ No

4- Misure di sicurezza

Quali delle seguenti misure di sicurezza sono applicate ai dati personali oggetto di trattamento?	4.1	□ Antimalware
	4.2	□ Sandbox
	4.3	□ Firewall/WAF
	4.4	□ Data Log
	4.5	> se no, sarebbe valutabile l'attivazione? _____
	4.6	□ IDS
	4.7	□ IPS
	4.8	□ Monitoraggio del traffico
	4.9	□ Sandbox
	4.10	□ Crittografia
	4.11	> se no, sarebbe valutabile l'attivazione? _____
	4.12	□ Pseudonimizzazione
	4.13	□ A.I.
	4.14	□ Scansione delle vulnerabilità
	4.15	□ Patching automatici
	4.16	□ 2FA
	4.17	□ VPN/SSL
		Sono implementate misure tecniche e organizzative per il controllo e la mitigazione dei rischi dagli attacchi cyber per impedire:
	4.18	□ Iniezione di codice
	4.19	□ Brute force
	4.20	□ XML External Entities (XXE)
	4.21	□ Security misconfigurations
	4.22	□ Cross Site Scripting (XSS)
	4.23	□ Sfruttamento di vulnerabilità o mancati aggiornamenti
	4.24	□ Mancato monitoraggio dei logs

5- Lista Sub-responsabili

1 Denominazione	
Servizio svolto	
ACN	□ SI (indicare link al catalogo ACN) ……..…… □ NO
2 Denominazione	
Servizio svolto	
ACN	□ SI (indicare link al catalogo ACN) ……..…… □ NO
3 Denominazione	
Servizio svolto	
ACN	□ SI (indicare link al catalogo ACN) …….. □ NO

Quanto sopra dichiarato potrà essere oggetto di verifica da parte del Titolare del trattamento.

Il sottoscritto _____ (legale rappresentante / delegato dal legale rappresentante) del soggetto giuridico..... con sede legale in ..... , dichiara di essere consapevole della responsabilità penale in caso di dichiarazioni mendaci, o di esibizione di atto falso o contenente dati non più rispondenti a verità ai sensi dell'articolo 76 del d.p.r. 28.12.2000 n.445

_____, _____

Firma

(da sottoscrivere digitalmente)

4.2 L' atto di nomina

Una volta individuato il fornitore cui affidare l'incarico, che abbia dimostrato di essere in grado di garantire un'adeguata protezione dei dati personali e di offrire garanzie sufficienti in termini di misure tecniche e organizzative, si procede alla formale nomina a Responsabile del trattamento, ai sensi dell'art. 28 del GDPR. La nomina costituisce il passaggio conclusivo del processo di selezione e ha la funzione di disciplinare in modo chiaro e vincolante i rapporti tra il Titolare del trattamento e il soggetto esterno incaricato.

L'atto di nomina rappresenta un addendum del contratto principale ed è a tutti gli effetti anch'esso un contratto di mandato, in cui il Titolare del trattamento indica le linee guida per la corretta gestione del dato al Responsabile esterno nominato. Detto contratto deve essere sottoscritto da entrambe le parti.

In conclusione, l'iter operativo da seguire è il seguente:

1. compilazione della checklist da parte del fornitore

2. analisi della stessa da parte del Titolare con il supporto del DPO,

3. affidamento dell'incarico

4. predisposizione e sottoscrizione dell'atto di nomina a Responsabile del trattamento.

Atto di nomina a responsabile esterno del trattamento dei dati personali

Il Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), in qualità di titolare autonomo del trattamento dei dati personali, nella persona del Rappresentante legale pro tempore.

Premesso che:

- ai sensi dell'art. 4, punto 8 del Regolamento 679/2016 (GDPR) il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del titolare del tratta- mento;
- ai sensi dell'art. 28 Reg. UE 2016/679, il Titolare può proporre una persona fisica, una persona giuridica e qualsiasi altro ente, associazione od organismo quale responsabile al trattamento dei dati che sia nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo di sicurezza;
- tra il Titolare e il Fornitore è stato stipulato il contratto di servizi n. ..... della durata di ..... (o con scadenza al .....);

- è intenzione del Titolare consentire l'accesso, sia al responsabile che alle persone autorizzate al trattamento, ai soli dati personali la cui conoscenza è necessaria per adempiere ai compiti attribuiti con il contratto di servizi;
- che il Fornitore possiede adeguati requisiti di esperienza, capacità e affidabilità sufficienti per mettere in atto misure tecniche e organizzative adeguate e per svolgere il ruolo di responsabile esterno del trattamento dei dati personali

Tutto quanto premesso,

NOMINA

Responsabile esterno del trattamento dei dati (di seguito Responsabile) l'ente ....., con sede legale ..... in persona del legale rappresentante pro tempore.

La società ....., in qualità di responsabile del trattamento, è tenuta a trattare i dati personali nel rispetto dei principi del Reg. UE 2016/679 e a rispettare le istruzioni impartite dal titolare del trattamento.

***

In ragione del contratto di servizi in essere tra le parti, occorre che venga svolto il trattamento dei seguenti dati personali:

- .....
- .....

La società.....è tenuta a:

1) trattare i dati nel rispetto dei principi di cui al Regolamento UE 2016/679 e solo per le finalità indicate nel contratto;
2) trattare i dati secondo le istruzioni documentate fornite dal Titolare del trattamento dei dati in allegato alla presente scrittura o con comunicazioni successive, che fanno parte integrante della presente nomina;
3) garantire che le persone autorizzate al trattamento dei dati personali siano state vincolate da un patto di riservatezza o abbiano, in ragione della loro funzione e dei loro titoli professionali, un obbligo legale di riservatezza e abbiano ricevuto una adeguata formazione in materia di protezione dei dati personali;
4) predisporre e tenere aggiornato, ai sensi dell'art. 30, par. 2 Reg. UE 20916/679, il registro delle attività di trattamento, come responsabile del trattamento;
5) adottare le misure di cui all'art. 32 Reg. UE 2016/679, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura dei dati trattati, dell'oggetto del servizio, delle finalità del trattamento, che comprendono, tra le altre, se del caso: *i)* la pseudonimizzazione e la cifratura dei dati persona- li, *ii)* la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di tratta- mento, *iii)* la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, *iv)* la procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di assicurare la sicurezza del trattamento;
6) assistere il titolare del trattamento, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste dell'interessato ai sensi degli artt. 15 a 22 Reg. UE 2016/679, con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile;

7) mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente accordo o contratto e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;
8) informare tempestivamente il Titolare sulla natura ritenuta illecita di alcune istruzioni ricevute dal titolare stesso, perché in contrasto con il Regolamento UE 29016/679 o altra norma di legge italiana o dell'Unione, relativa al trattamento dei dati;
9) informare e coinvolgere tempestivamente il Titolare qualora il Responsabile subisca un Data Breach;
10) assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36, GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
11) al momento della cessazione del contratto di servizi, cancellare o restituire tutti i dati personali trattati, in base a quanto richiesto dal titolare, oltre che cancellare la copia dei predetti dati, salvo che per la natura dell'incarico, viga una norma di legge che gli imponga la conservazione.

Col presente contratto, il Titolare conferisce autorizzazione scritta generale al Responsabile a poter ricorrere a eventuali ulteriori responsabili del trattamento ("sub-responsabile/i"), nella prestazione del Servizio.

Nel caso in cui il Responsabile faccia effettivo ricorso a sub-responsabili, il Responsabile medesimo si impegna a selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in

modo tale che il trattamento soddisfi i requisiti di cui alla normativa pro tempore applicabile e garantisca la tutela dei diritti degli interessati.

Il Responsabile del trattamento non ricorre ad un altro Responsabile se non previa aver comunicato i dati del sub-responsabile al Titolare del trattamento.

Il Responsabile è consapevole che, ai sensi dell'art. 82, comma 2 del Regola- mento (UE) 679/2016 ("Regolamento" o "GDPR"), lo stesso risponde per il danno causato dal trattamento se non adempie agli obblighi previsti dal Regola- mento specificatamente diretti ai Responsabili del trattamento (ai sensi dell'art. 28 del GDPR) o agisce in modo difforme o contrario rispetto alle istruzioni ricevute, contenute nel presente Accordo.

Trova applicazione lo stesso principio, qualora sia il sub-responsabile ad omettere di adempiere o adempia in modo difforme rispetto a quanto impartitogli di- rettamente dal responsabile principale o dal titolare.

Con il presente contratto si intende espressamente revocare e sostituire ogni altro contratto o accordo tra le parti inerente al trattamento di dati personali.

In fede

Data, luogo .....

Il Titolare
Comune di Arvier

.....

Il Responsabile

.....

Responsabile del trattamento	Data nomina	Servizio erogato
		Elaborazione buste paga
		Commercialista
		Consulente IT

5. Amministratore di sistema

Con il provvedimento del 27 novembre 2008 (aggiornato il 29 giugno 2009), il Garante per la protezione dei dati personali ha provveduto a normare ruoli e responsabilità dell'Amministratore di sistema (AdS).

L' Amministratore di sistema è una **persona fisica** con competenze informatiche che gestisce, configura e mantiene i sistemi di elaborazione dati o singole componenti (server, reti, database, appliance di sicurezza, ecc.). Può operare **all'interno** dell'organizzazione (dipendente) o **all'esterno** (fornitore/consulente); la natura del rapporto non cambia la sostanza del ruolo, ma incide sulle best practices da adottare in relazione agli adempimenti da mettere in atto:

· Se l'AdS è interno: è necessario fornirgli policy dettagliate che descrivano procedure di accesso, tracciamento e sicurezza (artt. 29 e 32 GDPR).

· Se l'AdS è esterno: le istruzioni possono confluire nell'atto di nomina da responsabile del trattamento (art. 28 GDPR) o in un allegato tecnico; il titolare deve conservare gli estremi identificativi di ciascun professionista che accede ai sistemi.

La scelta su chi deve ricoprire tale incarico spetta al Titolare del trattamento: prima di procedere alla nomina, infatti, egli dovrà verificare che l'AdS possieda adeguata **affidabilità professionale**, esperienza e know-how per l'incarico. Tale valutazione deve essere documentata, in conformità al principio di accountability.

Il titolare deve tenere un **elenco nominale** degli amministratori di sistema, con indicazione precisa delle **funzioni** e dei **privilegi** loro assegnati. Questo documento interno va mantenuto **costantemente aggiornato** e reso disponibile in caso di ispezioni da parte dell'Autorità.

Nome AdS	Azienda	Data di nomina

Lo scopo del registro consiste, da un lato, nel garantire che gli AdS lavorino nel rispetto delle misure di sicurezza definite; dall'altro lato, di garantire controlli periodici sui log di accesso.

Perché il monitoraggio sull'operato degli Amministratori di sistema sia effettivo – come richiesto dal provvedimento del Garante – il titolare deve garantire che ogni accesso ai sistemi e agli archivi elettronici venga registrato in modo puntuale: ogni log deve riportare **quando** l'Amministratore entra nel sistema, **quanto dura la sessione** e **quale operazione** (o comando) viene eseguita. Senza questi tre elementi il controllo risulta inefficace.

Il controllo sugli accessi logici può essere effettivamente esercitato solo se gli stessi siano dotati di determinate caratteristiche, all'uopo elencate nel Provvedimento del Garante:

· **Completezza:** il sistema di autenticazione deve tracciare non solo il tentativo di accesso, ma l'intera attività svolta dall'AdS finché rimane collegato.

· **Inalterabilità:** i file di log devono essere protetti da modifiche o cancellazioni; si ottiene con software di hardening o soluzioni di log management reperibili sul mercato.

· **Integrità:** la struttura tecnica adottata (firma digitale, hash, WORM storage, ecc.) deve permettere al titolare di verificare che il contenuto non sia stato manomesso.

Il titolare – o un delegato specifico – deve **revisionare i log almeno una volta l'anno** per accertare che non ci siano accessi sospetti. Un check più ravvicinato (trimestrale o semestrale) è consigliato in ambienti critici.

I log devono essere conservati per un periodo non inferiore a sei mesi; periodi più lunghi sono ammessi se coerenti con la valutazione dei rischi o con policy interne di sicurezza.

ATTO DI NOMINA DELL'AMMINISTRATORE DI SISTEMA

OGGETTO: Nomina dell'Amministratore di Sistema con riferimento alla protezione dei dati personali e alla gestione della sicurezza dei sistemi informatici.

---

1. PREMESSA

In qualità di Titolare del Trattamento ai sensi del Regolamento (UE) 2016/679 (GDPR) e del Decreto Legislativo 30 giugno 2003, n. 196 (Codice della Privacy), il **Comune di Arvier** intende nominare un Amministratore di Sistema incaricato di garantire la gestione e la sicurezza dei sistemi informatici aziendali, con particolare attenzione alla protezione dei dati personali trattati.

L'Amministratore di Sistema è un soggetto che, in virtù delle proprie competenze tecniche, ha il compito di gestire, monitorare e proteggere i sistemi informatici aziendali, al fine di garantire la sicurezza dei dati trattati e prevenire potenziali violazioni della privacy.

2. NOMINA

Con il presente atto, il Titolare del trattamento nomina:

[Nome completo dell'Amministratore di Sistema]
Posizione: [Inserire posizione aziendale]

come Amministratore di Sistema responsabile della gestione e della sicurezza dei sistemi informatici aziendali.

3. OBBLIGHI E RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

L'Amministratore di Sistema ha i seguenti obblighi e responsabilità in materia di protezione dei dati personali:

3.1 Gestione della Sicurezza Informatica

- Garantire l’adozione di adeguate misure di sicurezza fisiche, logiche e procedurali per la protezione dei dati personali trattati tramite i sistemi aziendali.
- Monitorare e controllare costantemente l'accesso ai sistemi informatici, con particolare attenzione alla gestione degli account utente e dei privilegi di accesso.
- Assicurare che l'accesso ai dati personali sia limitato ai soli soggetti autorizzati in base ai principi di necessità e proporzionalità.
- Garantire la gestione delle password aziendali e l'adozione di politiche per l’utilizzo sicuro delle stesse (ad esempio, password sicure e periodiche modifiche).

3.2 Monitoraggio e Audit

- Eseguire attività di audit periodiche per verificare l’integrità, la sicurezza e il corretto funzionamento dei sistemi informatici, con particolare attenzione alla gestione dei dati personali.
- Monitorare gli accessi e le operazioni sui dati personali, per individuare eventuali anomalie, violazioni o tentativi di accesso non autorizzato.
- Garantire la registrazione e la conservazione dei log di sistema per un periodo di tempo appropriato, in conformità alle normative sulla protezione dei dati.

3.3 Gestione degli Incidenti di Sicurezza

- Segnalare tempestivamente al Titolare del trattamento e al Responsabile della protezione dei dati (DPO) eventuali incidenti di sicurezza che possano compromettere la protezione dei dati personali.
- Collaborare con il DPO e le autorità competenti in caso di violazione dei dati personali, supportando le indagini e le misure di rimedio.

3.4 Formazione e Sensibilizzazione

- Collaborare con il DPO per l’adozione di attività di sensibilizzazione e formazione in materia di protezione dei dati personali, rivolte a tutti i dipendenti e collaboratori aziendali.
- Garantire che tutti gli utenti dei sistemi informatici aziendali siano informati riguardo le politiche di sicurezza informatica, in particolare per quanto riguarda la protezione dei dati personali.

3.5 Conformità alle Normative

- Assicurare che tutte le operazioni svolte sui sistemi informatici aziendali siano conformi alla normativa vigente in materia di protezione dei dati personali (GDPR, Codice Privacy, leggi nazionali e europee in materia di cybersecurity).
- Collaborare con il DPO per l'analisi d'impatto sulla protezione dei dati (DPIA) in caso di trattamenti che possano comportare rischi elevati per i diritti e le libertà degli interessati.

4. DURATA DELLA NOMINA

La presente nomina ha validità a partire dalla data di sottoscrizione e durerà fino a revoca esplicita, che potrà avvenire in qualsiasi momento da parte del Titolare del trattamento, previa comunicazione scritta.

5. CONTROLLI E VERIFICHE

L'Amministratore di Sistema è tenuto a sottoporsi a controlli e verifiche periodiche da parte del Titolare del trattamento per assicurare che tutte le disposizioni di cui al presente atto siano rispettate.

6. OBBLIGHI DI RISERVATEZZA

L'Amministratore di Sistema è tenuto a rispettare l'obbligo di riservatezza riguardo le informazioni e i dati trattati, anche successivamente alla cessazione del proprio incarico, e a garantire che tutti i dati trattati non vengano divulgati a terzi non autorizzati.

7. FIRME

Il presente atto è redatto in duplice copia, una delle quali viene trattenuta dal Titolare del trattamento e l'altra dall'Amministratore di Sistema.

Per accettazione:

Comune di Arvier
[Firma]
Data: [Inserire data]

[Nome dell'Amministratore di Sistema]
[Firma]
Data: [Inserire data]

6.Registro delle attività di trattamento – art. 30 GDPR

L'art. 30 del Regolamento UE 679/2016 prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.

Il registro dei trattamenti è un documento che contiene tutte le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento. Esso non è un adempimento meramente formale, ma un **documento dinamico che consente di mappare in modo sistematico tutte le attività di trattamento** dei dati personali svolte dall'Ente, identificando per ciascuna di esse le **finalità perseguite, le basi giuridiche, le categorie di dati e interessati coinvolti, i soggetti destinatari, i tempi di conservazione e le misure tecniche e organizzative adottate.**

Per le pubbliche amministrazioni, la tenuta del registro è **obbligatoria** ai sensi dell'art. 30, par. 5 del GDPR, anche nel caso in cui l'Ente non raggiunga i limiti dimensionali indicati per i soggetti privati. L'obbligo è stato inoltre ribadito dal Garante per la protezione dei dati personali nelle sue Linee Guida e nelle attività ispettive svolte a partire dal 2018.

Sotto il profilo operativo, il registro deve essere **tenuto per iscritto**, anche in formato elettronico, e **costantemente aggiornato**. Ogni modifica rilevante nell'organizzazione, nei sistemi informativi o nelle procedure che implichino il trattamento di dati personali deve essere riflessa nel registro. Il contenuto minimo è definito dal GDPR, ma l'Ente può arricchirlo con ulteriori informazioni utili per l'analisi dei rischi o la definizione delle misure di sicurezza.

Il registro costituisce, infine, un documento esibibile in caso di accertamenti da parte dell'Autorità Garante e rappresenta la base documentale per qualunque azione di valutazione, progettazione o revisione in ambito privacy.

Di seguito si riporta un esempio:

Tipologia di trattamento	**Natura dei dati trattati**	**Finalità del trattamento**	**Basi giuridiche**	**Categorie di interessati**	**Categorie di destinatari**	**Trasferimento dati extra UE**	**Termini ultimi previsti per la cancellazione**	**Misure di sicurezza tecniche e organizzative**
Attività di trattamento	- dati di contatto - dati particolari ex art 9 GDPR	A cosa serve il trattamento ?	- art 6 - art 9 - ulteriori basi giuridiche	- investitori - clienti - personale	Ulteriori soggetti a cui vengono inviati i dati	SI/NO	In ottemperanza alla normativa di settore	Misure informatiche o organizzative utilizzate a tutela dei dati personali

6.1 Registro dei responsabili

Secondo quanto stabilito dall'art 30, par. 2 GDPR, il responsabile del trattamento è tenuto a tenere un registro di "*tutte le categorie di attività relative al trattamento svolte per conto di un titolare*". Il contenuto obbligatorio di detto registro si compone dei seguenti requisiti:

A. Nome e dati di contatto del responsabile del trattamento, del titolare del trattamento per conto del quale il responsabile agisce, del rappresentante del titolare o del responsabile del trattamento e, ove possibile, del DPO;

B. Le categorie dei trattamenti effettuati per conto del titolare. A tal proposito è possibile indicare sul registro quanto riportato all'interno dell'atto di nomina a responsabile del trattamento. Ciò vale tanto per i responsabili quanto i sub-responsabili;

C. I trasferimenti dei dati personali verso paesi extra UE ovvero organizzazioni internazionali, con relativa identificazione del paese terzo/organizzazione internale. La descrizione dovrà essere

completata dalla documentazione comprovante le adeguate garanzie che il paese terzo/organizzazione internazionale mette in atto per la tutela dei dati personali.

D. Descrizione delle misure tecniche e organizzative di cui all'art 32 GDPR.

Se un soggetto ricopre il ruolo di responsabile del trattamento per conto di molteplici e distinti titolari, le informazioni obbligatorie di cui all'art 30, par 2 GDPR dovranno essere riportate all'interno del registro con riferimento a ciascuno dei titolari, suddividendo il registro in tante sezioni quanti sono i titolari per conto dei quali agisce. Se il numero di clienti titolari per i quali si agisce è ingente, al punto da rendere difficoltoso l'aggiornamento del registro, su quest'ultimo si potrebbe riportare il rinvio a collegamenti esterni quali potrebbero essere, ad esempio, schede o banche dati, contenenti la descrizione dei servizi forniti ai diversi titolari del trattamento.

Di seguito si riporta un esempio:

Categorie di trattamenti effettuati	**Titolare del trattamento**	**Trasferimenti extra UE**	**Misure tecniche e organizzative**
Attività di trattamento	AB Srl	NO	Misure informatiche o organizzative utilizzate a tutela dei dati personali
Attività di trattamento	CD Srl EF Spa	SI Specificare le garanzie a tutela dei dati personali	=

7.Data Breach – artt. 33-34 GDPR

L'art. 4 Reg. UE 679/2016 definisce un data breach 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*".

Nel parere 03/2014 il Gruppo di lavoro *ex* art. 29 ha chiarito che è possibile individuare diverse tipologie di violazioni di dati personali sulla base dei 3 principi che governano la sicurezza delle informazioni:

VIOLAZIONE DELLA RISERVATEZZA	**In caso di divulgazione dei dati personali e/ o nel caso di accesso non autorizzato o accidentale agli stessi**
VIOLAZIONE DELL'INTEGRITÀ	In caso di modifica non autorizzata o accidentale dei dati personali
VIOLAZIONE DELLA DISPONIBILITÀ	In caso di perdita, accesso o distruzione accidentale o non autorizzata di dati personali

7.1. Policy Data Breach

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque passaggi, di cui due eventuali

Fase	Contenuto	Azioni principali
1. Rilevazione e prima analisi	Al manifestarsi di un'anomalia o di una segnalazione interna/esterna, il titolare (o un delegato) avvia una **verifica preliminare** per accertare se l'evento integri effettivamente una violazione di dati personali.	– Raccolta delle evidenze tecniche e organizzative.– Classificazione provvisoria dell'incidente.
2. Valutazione d'impatto e contenimento	Una volta confermato il data breach, il titolare valuta: a) quali misure immediate siano idonee a **limitare o ridurre i danni** (es. ripristino da backup, segmentazione della rete, reset credenziali); b) se la violazione generi **rischio** o **rischio elevato** per i diritti e le libertà delle persone fisiche.	– Implementazione delle misure tecniche/organizzative di urgenza.– Identificazione dei soggetti incaricati del contenimento.– Decisione sull'obbligo di notifica al Garante (art. 33) e sulla necessità di comunicazione agli interessati (art. 34).
3. Notifica all'Autorità di controllo *(eventuale)*	Se la violazione può comportare un **rischio** per gli interessati, il titolare invia notifica al Garante **senza ingiustificato ritardo** e, ove possibile, entro **72 ore** dalla conoscenza dell'evento, motivando eventuali ritardi (art. 33 GDPR).	– Compilazione modulo ufficiale di notifica.– Trasmissione tramite i canali indicati dall'Autorità.– Archiviazione della prova di invio.
4. Comunicazione agli interessati *(eventuale)*	Qualora il rischio sia **elevato**, il titolare informa gli interessati **senza ingiustificato ritardo**, salvo che ricorra una delle eccezioni previste dall'art. 34 (adozione di misure di cifratura, successive misure	– Redazione di avviso chiaro e comprensibile.– Scelta del canale di comunicazione diretto o, in caso di esonero, pubblica informativa

Fase	Contenuto	Azioni principali
	mitigative, comunicazione sproporzionata).	equivalente.
5. Registrazione dell'incidente	A prescindere dall'obbligo di notifica o di comunicazione, ogni violazione deve essere **documentata** in un registro interno dei data breach (art. 5 par. 2 – principio di responsabilizzazione).	– Inserimento di dati descrittivi: natura dell'incidente, cause, categorie e volume dei dati coinvolti, misure adottate, esiti dell'analisi.– Conservazione del registro ai fini di eventuali verifiche dell'Autorità.

7.2. Registro Data Breach

Si riporta di seguito, a titolo di esempio, un modello di registro data breach.

REGISTRO DATA BREACH

Ai sensi del D.lgs 196/2003, del Regolamento UE 2016/679 e del D.Lgs n. 101/2018.

Il Titolare del trattamento è il Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), C.F. 80003210079 / P.IVA 00140870072, protocollo@pec.comune.arvier.ao.it

Comune di Arvier			**Violazione dei dati personali (Data Breach)**					
n.	**Data Evento**	**Tipo di evento**	**Natura dei dati coinvolti**	**Categoria dei soggetti interessati dal data breach**	**Valutazione del data breach** **Alto** **Medio** **Basso**	**Provvedimenti adottati**	**Comunicazione dal garante effettuata in data**	**Comunicazione agli interessati**

1		Alla data attuale non risultano evidenze di eventi annotabili nel presente registro.								

Documento firmato digitalmente:

Comune di Arvier

(DPO) I&P Partners Srl

8. Protocollo informatico, Albo Pretorio online e Trasparenza

Nel rispetto degli obblighi normativi che impongono alla pubblica amministrazione forme di pubblicità legale e trasparenza, l'Ente tratta dati personali anche attraverso tre strumenti principali: il **protocollo informatico**, l'**Albo Pretorio online** e la sezione **Amministrazione Trasparente** del proprio sito istituzionale.

1. Protocollo informatico
Ai sensi dell'art. 53 del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), l'Ente utilizza un sistema di protocollo informatico che consente la registrazione, classificazione e tracciabilità dei documenti ricevuti o formati. In conformità alle **Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici**, i **metadati associati ai documenti protocollati** sono conservati per un periodo di **trent'anni** e gli accessi al sistema sono sottoposti a **controlli e restrizioni**, in linea con le misure di sicurezza previste dall'art. 32 del GDPR. L'accesso è consentito esclusivamente agli incaricati, sulla base dei profili autorizzativi interni.

2. Albo Pretorio online
L'art. 32 della Legge 69/2009 stabilisce che gli atti destinati alla pubblicazione debbano essere resi disponibili sul sito istituzionale dell'Ente, nella sezione **Albo Pretorio online**, per garantire la

trasparenza e la pubblicità degli atti amministrativi. Tuttavia, la pubblicazione deve sempre avvenire nel **rispetto dei principi di minimizzazione e pertinenza dei dati**, come stabilito dagli artt. 5 e 6 del GDPR. Pertanto, qualora siano presenti dati personali non necessari o eccedenti rispetto alle finalità di pubblicazione, l'Ente procede all'**anonimizzazione o pseudonimizzazione** delle informazioni, al fine di tutelare i diritti degli interessati.

3. Amministrazione Trasparente
L'Ente è soggetto agli obblighi di pubblicazione previsti dal D.Lgs. 33/2013 in materia di trasparenza, integrità e prevenzione della corruzione. Le modalità di pubblicazione e di eventuale mascheramento dei dati personali sono regolate, tra l'altro, dalla **Deliberazione ANAC n. 1310/2016**, la quale stabilisce le **tabelle di pubblicazione** e i **criteri di oscuramento** o anonimizzazione dei dati, in base al bilanciamento tra interesse pubblico alla conoscibilità e tutela della riservatezza. L'Ente applica tali indicazioni nell'ambito della propria attività di aggiornamento della sezione "Amministrazione Trasparente", garantendo la pubblicazione di quanto richiesto dalla normativa, ma con attenzione costante alla **protezione dei dati personali**.

Nel loro insieme, tali strumenti comportano trattamenti sistematici di dati personali, spesso anche di natura particolare o giudiziaria. Per questo motivo, il personale coinvolto nelle attività di protocollo, pubblicazione e gestione dei contenuti online è **formato e autorizzato** in base a policy interne e istruzioni operative, e le attività sono tracciate conformemente al principio di accountability (art. 5, par. 2 GDPR).

9. Gestione del personale dipendente pubblico

Il trattamento dei dati dei dipendenti avviene per l'esecuzione del rapporto di pubblico impiego, e quindi necessario all'assolvimento di obblighi contrattuali conseguenti all'instaurazione e al mantenimento del rapporto di lavoro. I dati oggetto di trattamento sono:

- Dati anagrafici: nome, cognome, luogo e data di nascita, C.F.
- Dati di contatto: indirizzo posta elettronica, residenza e/o domicilio, numero di telefono
- Dati bancari: IBAN
- Dati particolari ex art 9 GDPR: salute, appartenenza sindacale, origini etniche/razziali
- Dati giudiziari ex art 10 GDPR

9.1. Informativa dipendenti

Ai sensi dell'art. 13 Reg. UE 679/2016, il titolare del trattamento ha l'obbligo di fornire al dipendente un'informativa, all'interno della quale vengono individuate tutte le informazioni, con riferimento ai dati personali del lavoratore e dei suoi familiari, strettamente necessarie per l'instaurazione e/o la gestione del rapporto di lavoro. La stessa deve essere consegnata al momento dell'assunzione.

INFORMATIVA PER I DIPENDENTI

La presente informativa è redatta da **Comune di Arvier**, allo scopo di informarLa riguardo il trattamento dei dati personali raccolti nell'ambito dell'attività lavorativa e del rapporto di lavoro con Lei in essere. La invitiamo a prendere atto delle informazioni di seguito riportate.

Dati del titolare del trattamento e del Data Protection Officer - DPO

Il titolare del trattamento è Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), C.F. 80003210079 / P.IVA 00140870072, protocollo@pec.comune.arvier.ao.it

Il titolare del trattamento ha provveduto a nominare un Responsabile Protezione Dati (RPD)/ Data Protection Officer (DPO), individuabile nella persona fisica del Dott. Ivano Pecis, e contattabile all'indirizzo mail dpo@prtnerprivacy.it

Tipologia di dati trattati

L'Ente raccoglie e tratta dati personali che possono includere, a titolo esemplificativo:

- Dati identificativi e di contatto: nome, cognome, codice fiscale, indirizzo di residenza, numero di telefono, indirizzo email.
- Dati inerenti il rapporto di lavoro: mansione, retribuzione, orari di lavoro, presenze, assenze, qualifiche, esperienze professionali.
- Dati bancari e finanziari: numeri di conti correnti, IBAN
- Dati fiscali e previdenziali: informazioni relative alla busta paga, trattenute fiscali, contributi previdenziali, imposte.
- Dati particolari ex art 9 GDPR: salute, appartenenza sindacale, convinzioni politiche, filosofiche o religiose, origini razziali o etniche.

Finalità del trattamento

I dati personali verranno trattati per le seguenti finalità:

- Gestione del rapporto di lavoro: adempimento di obblighi contrattuali, gestione delle presenze, buste paga, ferie, permessi, ecc.

- Adempimento degli obblighi legali e fiscali: per l'elaborazione delle dichiarazioni fiscali, la gestione dei contributi previdenziali e le comunicazioni con le autorità fiscali.

Natura del conferimento

Il conferimento dei dati personali è obbligatorio, pertanto, il mancato o l'errato conferimento comporterà l'impossibilità di dar corso al contratto ed agli adempimenti connessi.

Base giuridica del trattamento

Il trattamento dei dati personali si basa su diverse basi giuridiche, tra cui:

- Esecuzione di un contratto (art 6, par 1, lett *b* GDPR) : per l'adempimento degli obblighi previsti dal contratto di lavoro.
- Obbligo legale (art 6, par 1, lett *c*): per adempiere a obblighi imposti dalla legge o da autorità competenti (ad esempio, in materia fiscale e previdenziale).

Destinatari dei dati

I dati personali potranno essere comunicati a:

- Enti pubblici: autorità fiscali, autorità giudiziarie, enti previdenziali e assicurativi, in ottemperanza agli obblighi di legge.
- Fornitori di servizi: consulenti esterni, software house, fornitori di servizi bancari o finanziari.
- Soggetti interni all'Ente: i dati saranno accessibili solo a coloro che sono coinvolti nelle operazioni necessarie per l'adempimento delle finalità sopra indicate.

In nessun caso i Suoi dati saranno diffusi.

Tempi di conservazione dei dati personali

I dati personali verranno conservati per il periodo necessario a conseguire le finalità per le quali sono stati raccolti e, successivamente, per il periodo previsto dalla normativa vigente (ad esempio, per obblighi fiscali e previdenziali). I dati bancari e finanziari, in particolare, verranno trattati per il tempo necessario alla gestione delle operazioni finanziarie e successivamente archiviati in base agli obblighi di legge.

Trasferimento dei dati personali

Il Titolare del trattamento non trasferisce i dati personali in paesi terzi o a organizzazioni internazionali.

Diritti dell'interessato

Secondo quando disposto dal GDPR, i dipendenti possono esercitare i seguenti diritti relativamente al trattamento dei propri dati personali:

- Diritto di accesso: ottenere informazioni sui dati trattati dall'Ente e su come vengono utilizzati.
- Diritto di rettifica: correggere eventuali dati inesatti o incompleti.
- Diritto alla cancellazione (diritto all'oblio): chiedere la cancellazione dei propri dati, salvo vincoli legali.
- Diritto di opposizione: opporsi al trattamento dei dati in determinate circostanze.
- Diritto alla portabilità dei dati: ricevere i dati personali in un formato leggibile e trasferirli ad altri soggetti.
- Diritto di limitazione del trattamento: chiedere la limitazione dell'utilizzo dei propri dati in determinate situazioni.

Inoltre, nel caso in cui si ritenga che il trattamento sia stato svolto in violazione della normativa sulla protezione dei dati personali, è riconosciuto il diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 - Roma.

Firma del titolare del trattamento
Comune di Arvier

.....

Per presa visione
Firma del dipendente

.....

9.2. Corsi di formazione

La formazione del personale rappresenta un tassello essenziale per l'allineamento dell'Ente ai principi e alle prescrizioni del **Regolamento (UE) 2016/679**. Tale obbligo discende, in primo luogo, dall'**art. 29** GDPR, il quale stabilisce che il responsabile del trattamento – o chiunque operi sotto la sua autorità o sotto quella del titolare – **non può trattare dati personali se non previamente istruito** dal titolare stesso, salvo diversa previsione del diritto dell'Unione o degli Stati membri.

Il dovere formativo è richiamato altresì dall'**art. 32, par. 4**, che inserisce l'addestramento del personale tra le **misure tecnico-organizzative** necessarie per assicurare un livello di sicurezza adeguato al rischio. Ne consegue che il titolare e il responsabile del trattamento devono garantire che ogni soggetto autorizzato, avendo accesso a dati personali, **operi esclusivamente dopo aver ricevuto istruzioni appropriate**.

Per assolvere a tale onere, il titolare si affida a **professionisti con competenze specifiche in materia di protezione dei dati personali**, organizzando percorsi formativi rivolti a tutti i soggetti designati al trattamento. I corsi affrontano i seguenti aspetti:

- contenuti essenziali del GDPR e del quadro normativo nazionale;
- buone pratiche operative per prevenire o mitigare perdita, distruzione o accessi non autorizzati ai dati;
- procedure interne in caso di incidente, reclamo o esercizio dei diritti da parte degli interessati.

Al termine di ogni ciclo formativo viene somministrato un **test di verifica dell'apprendimento**; i relativi esiti vengono archiviati per attestare l'efficacia dell'attività svolta.

Data ultima formazione	Argomenti trattati	Soggetto relatore	Durata	Partecipanti	Attestati

10. Gestione dell'utenza

L'Ente effettua trattamenti di dati personali nell'ambito dell'erogazione dei propri servizi istituzionali attraverso **sportelli fisici e digitali**, sistemi di pagamento elettronico integrati (es. **PagoPA**) e nell'ambito delle prestazioni in materia di **servizi sociali**.

1. Sportelli fisici e digitali (e-Gov)
Attraverso gli sportelli tradizionali e i canali digitali di interazione con l'utenza, l'Ente raccoglie e tratta

dati personali ai fini del rilascio di **provvedimenti amministrativi** (es. concessioni, autorizzazioni, iscrizioni, agevolazioni). Tali trattamenti sono basati su **fondamenti giuridici previsti dalla legge o da un compito di interesse pubblico**, in conformità all'**art. 6, par. 1, lett. c) e e)** del GDPR. La raccolta dei dati avviene nel rispetto dei **principi di necessità, minimizzazione e pertinenza** (art. 5 GDPR) e può comportare la registrazione su sistemi elettronici o cartacei.

2. Trattamenti tramite PagoPA
L'Ente consente ai cittadini e agli operatori economici di effettuare pagamenti elettronici attraverso la piattaforma **PagoPA**, integrata con i **Prestatori di Servizi di Pagamento (PSP)** accreditati. In questo contesto, il trattamento dei **dati identificativi e di pagamento** avviene in modalità sicura, e i PSP operano **quali autonomi titolari del trattamento**, ai sensi dell'art. 4, punto 7, GDPR. L'Ente provvede, ove necessario, a rendere disponibile nei propri canali digitali il **link alla privacy policy del PSP utilizzato**, così da garantire trasparenza nei confronti dell'interessato, ai sensi degli artt. 13 e 14 GDPR.

3. Servizi sociali
Nell'ambito dei procedimenti riguardanti i servizi socio-assistenziali o socio-educativi, possono essere trattati **dati particolari** ai sensi dell'**art. 9 del GDPR**, relativi, ad esempio, allo stato di salute o alla condizione sociale degli interessati. Tali dati sono trattati esclusivamente **se strettamente indispensabili**, in osservanza del principio di **stretta necessità** previsto dall'**art. 2-sexies del D.Lgs. 196/2003**, come modificato dal D.Lgs. 101/2018. Ogni trattamento viene effettuato previa **adozione di misure tecniche e organizzative adeguate** per garantirne la riservatezza e la sicurezza, e nel rispetto delle **autorizzazioni normative specifiche** previste per la finalità perseguita.

In tutti i casi sopra indicati, il personale incaricato è **formato e autorizzato** in base alle disposizioni interne, e i trattamenti sono registrati nel **Registro delle attività di trattamento**, nel rispetto del principio di responsabilizzazione di cui all'art. 5, par. 2 del GDPR.

10.1 Informativa utenti

Per garantire la conformità al Regolamento (UE) 2016/679 (GDPR), il Comune, in qualità di Titolare del trattamento, ha il dovere di informare in modo chiaro e trasparente gli interessati – ossia i cittadini – circa le modalità con cui vengono trattati i dati personali che li riguardano. A tal fine, è necessario che ogni area e ufficio dell'Ente si doti di una specifica informativa sul trattamento dei dati, redatta in relazione alle peculiarità del servizio erogato. Tale informativa deve indicare, tra le altre cose, le finalità del trattamento, la base giuridica, le categorie di dati raccolti, i soggetti destinatari, i tempi di conservazione e i diritti riconosciuti agli interessati. L'adozione e la pubblicazione di informative puntuali rappresenta un elemento essenziale per assicurare trasparenza, responsabilizzazione e tutela effettiva dei diritti dei cittadini in materia di protezione dei dati personali.

10.2 Gestione delle richieste di esercizio dei diritti degli interessati

In conformità a quanto previsto dagli articoli **da 15 a 22 del Regolamento (UE) 2016/679,** gli interessati hanno il diritto di ottenere dal Titolare del trattamento, nei casi e nei limiti stabiliti dalla normativa vigente, l'accesso ai propri dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento, la portabilità dei dati, nonché di opporsi al trattamento e di non essere sottoposti a processi decisionali automatizzati, compresa la profilazione. L'esercizio di tali diritti è gratuito e può essere esercitato in qualsiasi momento, mediante richiesta rivolta al Titolare del trattamento attraverso i canali ufficiali dell'Ente (es. posta elettronica certificata, email istituzionale,

modulo cartaceo protocollato), ovvero al Data Protection Officer, secondo le modalità indicate nell'informativa pubblicata sul sito istituzionale.

Quali diritti?

- **Diritto di accesso (art. 15 GDPR)** – il diritto di ottenere conferma dell'esistenza del trattamento e copia dei dati, unitamente a tutte le relative informazioni (finalità, categorie, destinatari, tempi, diritti, origine dei dati, logica di eventuali decisioni automatizzate),
- **Diritto di rettifica (art. 16 GDPR)** – il diritto di ottenere la correzione o integrazione dei dati inesatti o incompleti senza ingiustificati ritardi .
- **Diritto di cancellazione ("diritto all'oblio", art. 17 GDPR)** – il diritto di ottenere la cancellazione dei dati personali quando non più necessari, in caso di revoca del consenso, trattamento illecito o opposizione, salvo casi di prevalente interesse pubblico, obblighi legali o difesa di diritti in sede giudiziaria
- **Diritto di limitazione del trattamento (art. 18 GDPR)** – il diritto di ottenere il blocco del trattamento (con conservazione dei dati ma interruzione dell'ulteriore trattamento) in specifiche ipotesi: contestazione dell'esattezza, trattamento illecito, o opposizione in attesa della verifica delle basi giuridiche.
- **Diritto alla portabilità dei dati (art. 20 GDPR)** – il diritto di ricevere i dati forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli ad un altro Titolare quando il trattamento si basa su consenso o contratto.
- **Diritto di opposizione (art. 21 GDPR)** – il diritto di opporsi in qualsiasi momento al trattamento fondato su legittimo interesse o finalità di interesse pubblico, nonché al trattamento a fini di marketing diretto; il Titolare può proseguire solo se dimostra motivi legittimi cogenti.
- **Diritto a non essere sottoposti a decisioni automatizzate (art. 22 GDPR)** – il diritto di non subire decisioni basate unicamente su processi automatizzati, incluse profilazioni, che producano effetti giuridici o incidano significativamente sulla persona, salvo casi eccezionali (necessità contrattuale, autorizzazione normativa, consenso esplicito)

L'Ente, in qualità di Titolare del trattamento, è tenuto a fornire **un riscontro all'interessato entro un termine massimo di trenta giorni dalla ricezione della richiesta**, prorogabile nei casi previsti dall'art. 12, par. 3 del Regolamento (UE) 2016/679, previa adeguata motivazione. Nei casi in cui il trattamento sia basato sul consenso, l'interessato ha altresì il diritto di revocarlo in qualsiasi momento, senza pregiudicare la liceità del trattamento effettuato prima della revoca stessa. In caso di mancato riscontro o di risposta insoddisfacente da parte dell'Ente, l'interessato ha facoltà di proporre reclamo all'Autorità Garante per la protezione dei dati personali, ai sensi dell'art. 77 del Regolamento (UE) 2016/679 e dell'art. 140-bis del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.

10.2. A. Procedura di presentazione delle richieste

Modulo per l'esercizio dei diritti ai sensi del Regolamento UE 2016/679 (GDPR)

Comune di Arvier
via Corrado Gex 8,11011, Arvier (AO)
C.F. 80003210079 / P.IVA 00140870072
protocollo@pec.comune.arvier.ao.it

1. DATI DELL'INTERESSATO

Cognome e Nome: .....
Data e luogo di nascita:.....
Codice fiscale: .....
Indirizzo di residenza: .....
Telefono: .....
Email: .....

In caso di esercizio dei diritti da parte di un delegato:
Nome del delegato: .....
Qualifica / relazione con l'interessato: .....

Allegare copia della delega e documento d'identità del delegato.

2. OGGETTO DELLA RICHIESTA

Il sottoscritto, ai sensi degli articoli **15-22 del Regolamento UE 2016/679**, intende esercitare i seguenti diritti in relazione al trattamento dei propri dati personali:

☐ Accesso ai dati personali (art. 15)
☐ Rettifica dei dati inesatti o integrazione (art. 16)
☐ Cancellazione dei dati personali ("diritto all'oblio", art. 17)
☐ Limitazione del trattamento (art. 18)
☐ Opposizione al trattamento (art. 21)
☐ Portabilità dei dati (art. 20)
☐ Revoca del consenso precedentemente prestato
☐ Reclamo al Garante per la Protezione dei Dati Personali
☐ Altro (specificare): .....

3. MOTIVAZIONE

Si prega di fornire eventuali dettagli utili a valutare la richiesta (es. periodo di riferimento, tipo di dati, servizio coinvolto, ecc.):

4. DOCUMENTAZIONE ALLEGATA

☐ Copia del documento di identità
☐ Eventuale delega e documento del delegato
☐ Ulteriore documentazione (specificare): .....

5. MODALITÀ DI RISPOSTA RICHIESTA

☐ Email
☐ PEC
☐ Raccomandata A/R
☐ Ritiro presso la sede dell'Ente (su appuntamento)

Luogo e data .....

Firma dell'interessato/delegato: .....

Informazioni ai sensi dell'art. 12 del GDPR

Il Titolare del trattamento si impegna a fornire riscontro alla presente richiesta **entro 30 giorni** dalla sua ricezione, salvo proroga in casi complessi, che verrà debitamente comunicata. In caso di rifiuto o mancato riscontro, l'interessato può rivolgersi al **Garante per la Protezione dei Dati Personali**.

10.2.B Modello di registro delle richieste

Numero richiesta	1	2	3	4
Addetto alla gestione della richiesta				
Data di ricezione della richiesta				
Dati identificativi dell'istante				
Dati di contatto dell'istante				
Tipologia richiesta				
Ricevibilità richiesta (ricevibile, ricevibile con integrazione, irricevibile)				
Eventuale data e contenuto della richiesta di integrazione				

Evasione della richiesta (data e contenuto)				
Costi sostenuti				
Contributo spese richiesto all'interessato				
Contributo spese versato dall'interessato				
Note				

11. Gestione dei fornitori

Nell'ambito dei rapporti contrattuali e precontrattuali instaurati con fornitori di beni e servizi, il Titolare del trattamento procede al trattamento dei dati personali riferibili a **persone fisiche operanti in nome e per conto dei fornitori stessi**, nonché, ove applicabile, ai dati personali di ditte individuali o professionisti. Tali trattamenti sono effettuati nel rispetto dei principi di liceità, correttezza e trasparenza, ed esclusivamente per finalità connesse alla gestione del rapporto contrattuale, all'esecuzione di obblighi derivanti da disposizioni di legge e alla corretta organizzazione delle attività dell'Ente.

In particolare, i dati personali sono trattati per **finalità amministrativo-contabili e gestionali**, quali: compilazione e aggiornamento delle anagrafiche dei fornitori, gestione degli ordini, emissione e ricezione di fatture, registrazioni contabili, adempimenti fiscali e tributari, gestione dei pagamenti, fissazione di appuntamenti, gestione delle comunicazioni operative, nonché per l'esecuzione di ogni altra attività connessa o strumentale all'esecuzione delle prestazioni oggetto del contratto. Il trattamento può avvenire sia con strumenti cartacei che elettronici e telematici, nel rispetto delle misure di sicurezza previste dall'art. 32 del Regolamento (UE) 2016/679.

La **base giuridica** del trattamento è costituita dall'**esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato (art. 6, par. 1, lett. b) del GDPR), nonché dall'adempimento di obblighi di legge cui è soggetto il Titolare (art. 6, par. 1, lett. c)).** I dati potranno essere comunicati esclusivamente ai soggetti legittimati ai sensi di legge o a responsabili esterni del trattamento previamente nominati, qualora coinvolti nella gestione dei servizi.

Il Titolare assicura che i dati non saranno oggetto di diffusione e che saranno conservati per il tempo strettamente necessario al perseguimento delle finalità sopra indicate, nel rispetto dei termini previsti dalle normative civilistiche, fiscali e tributarie vigenti.

11.1 Informativa

INFORMATIVA PER I FORNITORI

In conformità del Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Reg. UE del Parlamento europeo e del Consiglio del 27 aprile 2016, n. 679 – GDPR), **Comune di Arvier** (di seguito "l'Ente"), in qualità di "Titolare del trattamento", desidera informarLa che tratterà i dati personali che la riguardano ai sensi degli artt. 13 e 14 del succitato Regolamento.

Dati del titolare del trattamento e del Data Protection Officer - DPO

Il titolare del trattamento è Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), C.F. 80003210079 / P.IVA 00140870072, protocollo@pec.comune.arvier.ao.it

Il titolare del trattamento ha provveduto a nominare un Responsabile Protezione Dati (RPD)/ Data Protection Officer (DPO), individuabile nella persona fisica del Dott. Ivano Pecis, e contattabile all'indirizzo mail dpo@partnerprivacy.it

Tipologia di dati trattati

I dati oggetto di trattamento sono:

- Dati anagrafici (nome, cognome, codice fiscale del legale rappresentante, P.IVA);
- Dati di contatto (indirizzo di consegna, telefono, e- mail);
- Dati fiscali, bancari e amministrativi
- Dati relativi ad incarichi e qualifiche

Finalità del trattamento

I dati personali da Lei forniti saranno trattati per finalità connesse:

a) all'esecuzione e alla gestione delle procedure di selezione, affidamento e stipula dei contratti;

b) alla tenuta della contabilità, alla fatturazione, all'effettuazione di comunicazioni sia con mezzi cartacei che informatici;

c) all’adempimento di obblighi legali previsti dalla normativa fiscale e tributaria;

Natura del conferimento

Il conferimento dei dati personali è obbligatorio, pertanto, il mancato conferimento comporterà l’impossibilità, da parte nostra, di dar corso al contratto ed agli adempimenti connessi.

Base giuridica del trattamento

 art 6, par. 1, lett b) GDPR: i dati da Lei raccolti verranno trattati per l’esecuzione di misure contrattuali

 Art 6, par 1, lett c) GDPR: i dati personali, a Lei direttamente o indirettamente riconducibili, verranno trattati per l’adempimento di obblighi legali, conformemente alla normativa nazionale e comunitaria.

In ogni caso i dati personali raccolti verranno trattati nel rispetto dei principi di liceità, correttezza e trasparenza e comunque in modo tale da garantirne la sicurezza e la massima riservatezza, conformemente a quanto disposto dall’art 5 Reg. Ue 679/2016.

Destinatari dei dati

I Suoi dati personali, potranno essere comunicati a soggetti terzi, per esigenze tecniche ed operative strettamente collegate alle finalità sopra enunciate ed in particolare alle seguenti categorie di soggetti:

a) enti, professionisti, società od altre strutture da noi incaricate dei trattamenti connessi all’adempimento degli obblighi amministrativi, contabili e gestionali legati all’ordinario svolgimento della nostra attività economica, anche per finalità di recupero credito;

b) alle pubbliche autorità ed amministrazioni per le finalità connesse all’adempimento di obblighi legali o ai soggetti legittimati ad accedervi in forza di disposizioni di legge, regolamenti, normative comunitarie;

c) banche, istituti finanziari o altri soggetti ai quali il trasferimento dei suddetti dati risulti necessario allo svolgimento dell'attività dell'Ente in relazione all'assolvimento, da parte nostra, delle obbligazioni contrattuali assunte nei Vostri confronti;

In nessun caso i Suoi dati saranno diffusi.

Tempi di conservazione dei dati personali

Conserveremo i Suoi dati personali in una forma che non consenta l'identificazione degli stessi per un arco temporale non superiore al conseguimento delle finalità per le quali i dati sono stati raccolti; verranno pertanto conservati fino all'esistenza del rapporto contrattuale in essere e non oltre i 10 anni a decorrere dalla cessazione del contratto ai sensi dell'art. **2946 c.c. – Prescrizione ordinaria** - mentre i dati personali strettamente necessari per gli adempimenti fiscali e contabili, venuta meno la finalità per la quale erano stati raccolti, verranno conservati per un periodo di 10 anni come sancito dall'art. **2220 c.c.**

Trasferimento dei dati personali

Il Titolare del trattamento non trasferisce i dati personali in paesi terzi o ad organizzazioni internazionali.

Diritti dell'interessato

In qualsiasi momento, gli interessati hanno il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento e la relativa cancellazione. È, altresì, possibile opporsi al trattamento e richiederne la limitazione.

Inoltre, nel caso in cui si ritenga che il trattamento sia stato svolto in violazione della normativa sulla protezione dei dati personali, è riconosciuto il diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 - Roma.

Firma del titolare del trattamento
Comune di Arvier

.....

Per presa visione
Firma del fornitore

.....

12. Gestione del sito istituzionale e dei servizi online

La gestione del sito internet istituzionale comporta, per il Titolare del trattamento, la possibilità di trattare dati personali degli utenti che accedono e interagiscono con i contenuti e i servizi offerti online. In conformità ai principi di liceità, correttezza e trasparenza sanciti dal Regolamento (UE) 2016/679, il Titolare è tenuto ad adottare specifiche misure organizzative e tecniche finalizzate a garantire la sicurezza, l'integrità e la riservatezza dei dati raccolti, prevenendo così il rischio di accessi non autorizzati, perdite, usi illeciti o non conformi alle finalità dichiarate. Nessun dato personale acquisito attraverso il servizio web potrà essere oggetto di diffusione o comunicazione non autorizzata, salvo nei casi espressamente previsti dalla normativa vigente.

URL	Hosting	Fornitore	Responsabile del sito	Aggiornamento privacy policy	Aggiornamento cookie policy	Cookie tecnici	Cookie analitici
INSERIRE							

12.1. Gestione dei cookie

Nel contesto della gestione del sito istituzionale, il Titolare del trattamento adotta specifiche misure in materia di utilizzo dei cookie e di altri strumenti di tracciamento, nel rispetto della normativa vigente e, in particolare, del Provvedimento n. 231 del 10 giugno 2021 adottato dal Garante per la protezione dei dati personali, nonché delle disposizioni del Regolamento (UE) 2016/679. I cookie sono stringhe di testo di piccole dimensioni che i siti web, direttamente o per il tramite di soggetti terzi, inviano e archiviano all'interno del terminale dell'utente al fine di garantire il corretto funzionamento del sito, migliorare l'esperienza di navigazione o per finalità di profilazione.

Esistono tre tipi di cookie:

1. Tecnici: impiegati esclusivamente per consentire la navigazione o per fornire all'utente un servizio esplicitamente richiesto. Non richiedono il consenso preventivo dell'interessato, ma devono essere

adeguatamente descritti all'interno della cookie policy.

2. Analitici: utilizzati per l'elaborazione di statistiche aggregate e anonime relative alla navigazione. Qualora detti strumenti siano configurati in modo da non consentire l'identificazione diretta dell'utente (ad esempio, mediante la mascheratura della quarta componente dell'indirizzo IP e il divieto di incrocio dei dati con ulteriori informazioni detenute da terzi), possono essere equiparati ai cookie tecnici e non richiedere il consenso.

3. Di profilazione: destinati a raccogliere informazioni utili a creare profili personalizzati dell'utente e inviare messaggi pubblicitari mirati. Non possono essere attivati in assenza di un consenso esplicito e documentato.

12.2 Form contatti

Tra le funzionalità messe a disposizione degli utenti rientra il modulo di contatto, attraverso il quale è possibile inviare richieste o comunicazioni all'Ente. La compilazione del form comporta necessariamente la raccolta e il successivo trattamento di dati personali identificativi e di contatto dell'interessato, così come specificati nei campi obbligatori e facoltativi del modulo stesso. Tali trattamenti sono effettuati esclusivamente per dare seguito alle istanze presentate dagli utenti e in esecuzione di misure precontrattuali adottate su richiesta dell'interessato, ai sensi dell'art. 6, par. 1, lett. b), del Regolamento (UE) 2016/679.

12.3 Informativa

In ottemperanza all'art. 13 del Regolamento (UE) 2016/679, il Titolare del trattamento garantisce la pubblicazione sul sito istituzionale di un'informativa specifica e facilmente accessibile, redatta in forma chiara e trasparente, relativa al trattamento dei dati raccolti attraverso il modulo di contatto. L'informativa contiene tutte le informazioni necessarie affinché l'interessato possa esercitare consapevolmente i propri diritti, conoscere le finalità del trattamento, i tempi di conservazione dei dati, le modalità del trattamento e gli eventuali destinatari.

All'interno dell'informativa vi deve essere una chiara elencazione dei dati trattati. Si riportano, a titolo d esempio:

- Dati anagrafici (nome e cognome)
- Dati di contatto (indirizzo mail, PEC, numero di telefono)
- Dati tecnici raccolti: cookie, indirizzo IP, Mac Address ecc

12.4 Iscrizione alla newsletter

Il servizio di newsletter rappresenta uno strumento di comunicazione periodica attraverso il quale il Titolare del trattamento informa gli utenti che ne abbiano fatto esplicita richiesta circa attività istituzionali, aggiornamenti, iniziative e altri contenuti di interesse. L'attivazione del servizio sul sito web comporta necessariamente il trattamento di dati personali degli utenti, in particolare dati identificativi e di contatto raccolti mediante l'apposito modulo di iscrizione.

Ai sensi dell'art. 13 del Regolamento (UE) 2016/679, il Titolare è tenuto a fornire agli interessati un'informativa completa e trasparente, pubblicata in calce al form di iscrizione e resa disponibile prima dell'invio della richiesta di adesione al servizio. L'informativa deve specificare le modalità del trattamento, le finalità perseguite, i tempi di conservazione dei dati, nonché i diritti esercitabili dall'interessato. La base giuridica del trattamento è rappresentata dal consenso libero, specifico, informato e inequivocabile dell'utente, ai sensi dell'art. 6, par. 1, lett. a) del Regolamento (UE) 2016/679. Tale consenso deve essere acquisito tramite un atto positivo inequivocabile (es. spunta volontaria di una casella), distinto da eventuali ulteriori finalità o servizi. L'utente potrà, in ogni momento, revocare il consenso prestato, senza pregiudicare la liceità del trattamento basato sul consenso prima della revoca, anche mediante appositi link di disiscrizione presenti in calce ad ogni comunicazione ricevuta.

Il Titolare assicura, altresì, che il trattamento dei dati raccolti per finalità di invio della newsletter avvenga nel rispetto dei principi di minimizzazione e limitazione della finalità, nonché mediante l'impiego di strumenti e misure tecniche idonee a garantire la sicurezza e la riservatezza dei dati trattati.

13. Misure di sicurezza

Il trattamento dei dati personali acquisiti attraverso il sito avviene mediante strumenti informatici e telematici, da parte di soggetti appositamente autorizzati, interni o esterni all'organizzazione del Titolare, nel rispetto dei principi di riservatezza e di limitazione del trattamento. A tal fine, il Titolare è tenuto ad adottare misure di sicurezza informatica adeguate al rischio, ai sensi dell'art. 32 del Regolamento (UE) 2016/679, al fine di assicurare la protezione dei dati da accessi illeciti o non autorizzati, nonché da eventi accidentali che possano comprometterne la disponibilità, l'integrità e la confidenzialità.

Si riportano, a titolo di esempio, alcune delle misure di sicurezza informatica da adottare per una corretta gestione e protezione dei dati personali trattati dall'Ente.

- **Cifratura** database sensibili;
- **Backup georidondante** settimanale;
- **Accesso** con autenticazione a due fattori (art. 6 CAD);
- **Penetration test annuale** (linee guida ACN sulla sicurezza ICT nella PA);
- **Business continuity** conforme a ISO 22301.

13.1.Sicurezza della rete

L'accesso a Internet da parte del personale interno è strumentale allo svolgimento delle attività istituzionali e operative dell'Ente e, pertanto, rientra nel contesto della prestazione lavorativa. In tale prospettiva, il Titolare del trattamento è tenuto a disciplinarne l'uso mediante apposite direttive interne,

nel rispetto dei principi di pertinenza e proporzionalità, così come previsto dal Regolamento (UE) 2016/679 e dallo Statuto dei Lavoratori, come modificato dal D.Lgs. 151/2015.

L'utilizzo della rete Internet deve avvenire esclusivamente per finalità connesse allo svolgimento delle mansioni lavorative e nel rispetto delle policy aziendali in materia di sicurezza informatica.

Ai fini della tutela della sicurezza del patrimonio informativo dell'Ente e della prevenzione di accessi non autorizzati, il Titolare del trattamento ha l'onere di adottare adeguate misure tecniche e organizzative, tra cui l'installazione di firewall, sistemi antivirus e strumenti di monitoraggio del traffico di rete. Tali dispositivi consentono di filtrare e controllare il traffico in entrata e in uscita secondo regole predefinite, riducendo i rischi derivanti da minacce informatiche e garantendo un'adeguata protezione dei dati trattati. L'eventuale attività di monitoraggio deve avvenire nel rispetto dei principi di necessità, proporzionalità e trasparenza, nonché previa adeguata informazione dei lavoratori ai sensi dell'art. 13 del Regolamento (UE) 2016/679 e dell'art. 4, comma 3, dello Statuto dei Lavoratori.

14. Social media

Il Comune si impegna ad adottare un apposito regolamento sull'utilizzo dei social media, finalizzato a disciplinare il corretto comportamento dei dipendenti e collaboratori nell'uso degli strumenti di comunicazione digitale, sia istituzionali sia personali, quando riconducibili all'attività dell'Ente. Tale regolamento definirà le modalità di gestione dei profili ufficiali del Comune, le regole di condotta per la pubblicazione dei contenuti e le misure necessarie a garantire il rispetto della normativa in materia di protezione dei dati personali e della privacy. L'obiettivo è promuovere una comunicazione pubblica trasparente, responsabile e coerente con i principi di imparzialità, decoro e tutela dell'immagine dell'Amministrazione.

15. Videosorveglianza

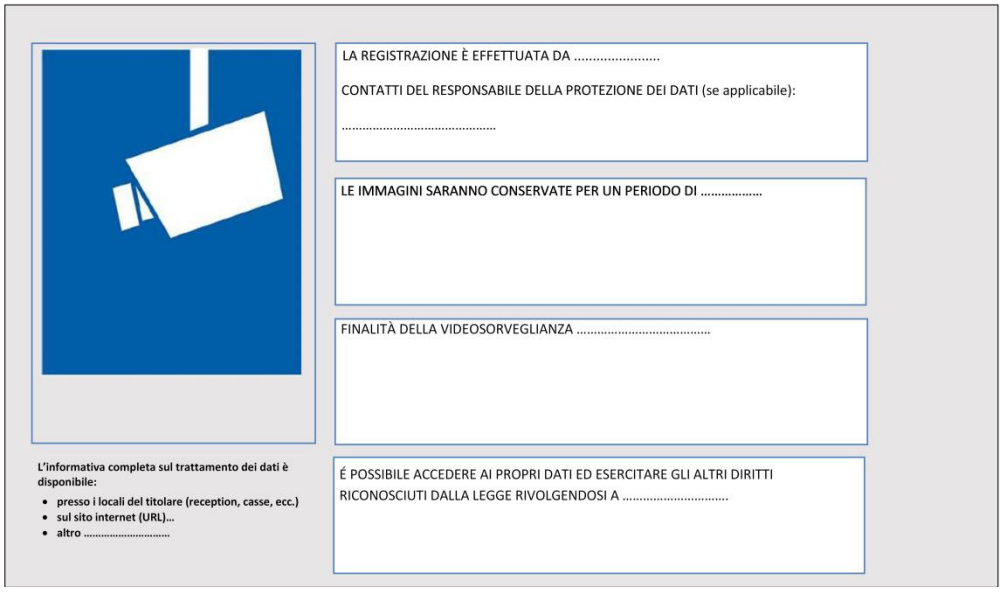
La gestione degli impianti di videosorveglianza deve avvenire nel pieno rispetto della normativa sulla protezione dei dati personali, in particolare il Regolamento UE 2016/679 (GDPR) e le indicazioni del Garante per la protezione dei dati. Per quanto riguarda le **telecamere interne, destinate ad ambienti di lavoro,** è necessario ottenere l'autorizzazione preventiva dell'Ispettorato Territoriale del Lavoro qualora la videosorveglianza possa avere finalità di controllo dei lavoratori. Contestualmente, il gestore dell'impianto deve fornire una relazione tecnica che descriva dettagliatamente il funzionamento del sistema, le modalità di registrazione e conservazione dei dati e le misure di sicurezza adottate, così da garantire la protezione dei dati trattati.

Per le telecamere esterne, utilizzate per la videosorveglianza territoriale, l'impianto deve essere disciplinato da un **regolamento aggiornato** che definisca le finalità del trattamento, le aree sorvegliate, le modalità di accesso alle registrazioni e i tempi di conservazione. Tale regolamento deve essere periodicamente verificato e aggiornato per rispondere a eventuali modifiche normative o operative. Inoltre, tutte le aree videosorvegliate devono essere corredate da **cartelli informativi** conformi ai parametri stabiliti dal Garante, chiaramente visibili e leggibili, che indichino le finalità della videosorveglianza e il soggetto titolare del trattamento.

MODELLO SEMPLIFICATO CARTELLO VIDEOSORVEGLIANZA

(EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020)

Per informazioni: www.garanteprivacy.it/faq/videosorveglianza



L'**informativa completa deve essere pubblicata sul sito web istituzionale** e includere tutte le informazioni richieste dal GDPR, comprese le categorie di dati trattati, le finalità, la base giuridica, i tempi di conservazione e le modalità di esercizio dei diritti degli interessati.

Deve essere redatta la **Valutazione d'Impatto sulla Protezione dei Dati (DPIA), come previsto dall'articolo 35 del GDPR**, al fine di valutare i rischi per i diritti e le libertà degli interessati. La DPIA deve essere supportata da una **relazione tecnica del gestore** dell'impianto, che illustri il funzionamento del sistema, le misure di sicurezza adottate, le modalità di protezione dei dati, l'accesso alle registrazioni e la loro conservazione. Tutti gli adempimenti descritti devono essere monitorati e aggiornati periodicamente, con evidenza documentale nel MOP, garantendo così la conformità normativa, la trasparenza nei confronti degli interessati e la gestione corretta e sicura di tutti gli impianti di videosorveglianza.

15.1. Informativa

Informativa sulla Videosorveglianza Territoriale

del Comune di Arvier

Premessa

Il Comune di Arvier, in qualità di Titolare del trattamento dei dati ai sensi del Regolamento (UE) 2016/679 (GDPR) e del Decreto Legislativo 30 giugno 2003, n. 196, così come novellato dal D.Lgs. 10 agosto 2018, n. 101 (Codice in materia di protezione dei dati personali), informa la cittadinanza circa l'installazione e l'utilizzo di un sistema di videosorveglianza sul proprio territorio comunale. L'implementazione di tale sistema avviene nel pieno rispetto dei principi di necessità, proporzionalità, liceità, correttezza e trasparenza, garantendo la minimizzazione dei dati e la protezione degli stessi fin dalla progettazione e per impostazione predefinita (privacy by design e privacy by default).

1. Finalità del Trattamento

Il sistema di videosorveglianza territoriale è installato ed utilizzato esclusivamente per il perseguimento delle seguenti specifiche e legittime finalità di interesse pubblico, così come definite dalla normativa vigente:

- **Tutela della sicurezza urbana:** prevenzione e contrasto di fenomeni di criminalità, vandalismo, danneggiamento di beni pubblici e privati, spaccio di sostanze stupefacenti, e altre condotte illecite.

- **Sicurezza della circolazione stradale:** monitoraggio del traffico, rilevamento di infrazioni al Codice della Strada (ad esempio, transito nelle zone a traffico limitato, sosta vietata, accesso abusivo a corsie preferenziali, nel rispetto delle specifiche normative e omologazioni per tali funzioni), gestione di eventi straordinari (es. incidenti).

- **Protezione dei beni comunali e del patrimonio pubblico:** salvaguardia di edifici, strutture, parchi, giardini, monumenti e altre infrastrutture di proprietà comunale da atti di degrado, danneggiamento o furto.

- **Prevenzione e repressione dell'abbandono illecito di rifiuti:** contrasto al fenomeno dell'abbandono di rifiuti solidi urbani e speciali sul territorio, mediante l'identificazione dei responsabili.

- **Collaborazione con le Forze di Polizia:** supporto alle attività di indagine e repressione di reati, su richiesta motivata e nei limiti stabiliti dalla legge.

Si precisa che le immagini non saranno utilizzate per finalità diverse da quelle sopra elencate e, in nessun caso, per il controllo a distanza dell'attività lavorativa dei dipendenti comunali o per l'indagine sulle abitudini private dei cittadini.

2. Base Giuridica del Trattamento

Il trattamento dei dati personali (immagini) raccolti tramite il sistema di videosorveglianza si fonda sulle seguenti basi giuridiche, ai sensi dell'articolo 6, paragrafo 1, del GDPR:

- **Art. 6, par. 1, lett. e) GDPR: "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".** Tale base giuridica trova fondamento nelle disposizioni normative che attribuiscono ai Comuni funzioni in materia di sicurezza urbana (es. D.L. 20 febbraio 2017, n. 14, convertito con modificazioni dalla L. 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città"), prevenzione e contrasto dell'abbandono dei rifiuti (es. D.Lgs. 3 aprile 2006, n. 152), gestione della circolazione stradale (D.Lgs. 30 aprile 1992, n. 285).

- **Art. 6, par. 1, lett. c) GDPR: "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento".** Questa base giuridica si applica in riferimento a specifiche normative che impongono o consentono l'adozione di misure di videosorveglianza per finalità ben definite (es. controllo del traffico veicolare per rilevazione infrazioni, laddove specificatamente normato e omologato).

3. Titolare del Trattamento e Responsabili del Trattamento

Il Titolare del trattamento è il Comune di Arvier, con sede in via Corrado Gex 8,11011, Arvier (AO), C.F. 80003210079 / P.IVA 00140870072, protocollo@pec.comune.arvier.ao.it

Il Responsabile della Protezione dei Dati (RPD/DPO) designato dal Comune è contattabile al seguente e-mail/PEC: dpo@partnerprivacy.it

La gestione tecnica e operativa del sistema di videosorveglianza potrebbe essere affidata a soggetti esterni qualificati, nominati quali Responsabili del Trattamento ai sensi dell'articolo 28 del GDPR. Tali nomine avverranno tramite contratti o altri atti giuridici che vincolino il Responsabile del Trattamento al Titolare, stabilendo la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. I Responsabili del Trattamento garantiranno il rispetto delle misure tecniche e organizzative adeguate per la protezione dei dati.

4. Categorie di Dati Personali Trattati

Il sistema di videosorveglianza tratta esclusivamente dati personali costituiti da immagini (videoriprese) che possono potenzialmente consentire l'identificazione di persone fisiche (es. volto, corporatura, abbigliamento, veicoli). Non è prevista l'acquisizione di dati biometrici, né l'associazione delle immagini ad altre informazioni personali (es. nomi, indirizzi, dati

sensibili) salvo quanto strettamente necessario per le finalità di indagine giudiziaria e previa autorizzazione dell'Autorità Giudiziaria.

5. Modalità del Trattamento e Misure di Sicurezza

Il trattamento dei dati avviene con strumenti elettronici e informatici. Vengono adottate misure di sicurezza tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, inclusi:

- **Accesso Selettivo:** L'accesso alle immagini registrate è strettamente limitato al personale autorizzato e debitamente formato (es. personale della Polizia Locale, dipendenti comunali specificamente incaricati e formati), identificato tramite credenziali personali e non cedibili.

- **Crittografia:** Le comunicazioni tra le telecamere e i sistemi di registrazione, nonché l'archiviazione dei dati, sono protette da meccanismi di crittografia ove tecnicamente fattibile.

- **Controllo degli Accessi Fisici:** I locali in cui sono conservati i sistemi di registrazione (DVR/NVR) sono protetti da accessi non autorizzati.

- **Registrazione dei Log:** Vengono tenuti registri degli accessi e delle operazioni effettuate sui sistemi di videosorveglianza, per consentire la verifica della legittimità degli accessi e dei trattamenti.

- **Mascheramento Aree Non Pertinenti:** Le telecamere sono posizionate e configurate per riprendere solo le aree strettamente necessarie al perseguimento delle finalità dichiarate. Ove possibile e tecnicamente attuabile, vengono oscurate (mascheramento dinamico) le aree non pertinenti o le proprietà private (es. interni di abitazioni, giardini privati).

- **Informativa visiva:** La presenza delle telecamere è segnalata da appositi cartelli informativi, chiaramente visibili in tutte le zone soggette a videosorveglianza, recanti le informazioni essenziali previste dalla normativa (finalità, Titolare, riferimento all'informativa completa).

6. Tempi di Conservazione dei Dati

Le immagini registrate sono conservate per il periodo strettamente necessario al perseguimento delle finalità per cui sono raccolte, e comunque per un periodo non superiore a sette giorni.

Decorso tale termine, le immagini vengono automaticamente e irrimediabilmente cancellate dai sistemi, salvo che debbano essere conservate per adempiere a un obbligo di legge o su specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria nell'ambito di indagini in corso. In tali casi, le immagini sono estratte dal sistema e conservate separatamente con misure di sicurezza adeguate.

7. Destinatari o Categorie di Destinatari dei Dati

I dati raccolti tramite il sistema di videosorveglianza possono essere comunicati, nei limiti strettamente necessari al perseguimento delle finalità sopra indicate e nel rispetto delle normative vigenti, alle seguenti categorie di soggetti:

- Forze di Polizia (Polizia di Stato, Carabinieri, Guardia di Finanza), su richiesta motivata e nei limiti delle loro funzioni istituzionali.

- Autorità Giudiziaria, su richiesta e nei limiti delle indagini in corso.

- Polizia Locale del Comune di Arvier, nell'esercizio delle proprie funzioni.

- Eventuali soggetti terzi (es. manutentori del sistema, società di vigilanza) nominati Responsabili del Trattamento, esclusivamente per le finalità di gestione e manutenzione del sistema e sotto stretto controllo del Titolare.

Non è prevista la diffusione dei dati a destinatari indeterminati.

8. Diritti degli Interessati

In qualità di interessato al trattamento, l'utente gode dei diritti previsti dagli articoli da 15 a 22 del GDPR, in particolare:

- **Diritto di accesso (Art. 15 GDPR):** Diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati e alle informazioni relative al trattamento. Data la natura del trattamento (immagini anonime o difficilmente riconducibili all'interessato se non in contesti specifici e per brevi periodi) e la finalità di sicurezza pubblica, l'esercizio del diritto di accesso potrebbe essere limitato nei casi e nei modi previsti dalla normativa, in particolare per non compromettere indagini o attività di prevenzione e repressione di reati.

- **Diritto di rettifica (Art. 16 GDPR):** Diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano.

- **Diritto alla cancellazione (Art. 17 GDPR):** Diritto di ottenere la cancellazione dei dati personali che lo riguardano, senza ingiustificato ritardo, salvo i casi previsti dall'art. 17, par. 3, GDPR.

- **Diritto di limitazione di trattamento (Art. 18 GDPR):** Diritto di ottenere la limitazione del trattamento quando ricorre una delle ipotesi previste dall'art. 18, par. 1, GDPR.

- **Diritto di opposizione (Art. 21 GDPR):** Diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano. Tuttavia, per i trattamenti basati sull'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, il Titolare potrà dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

- **Diritto di proporre reclamo all'Autorità di controllo (Art. 77 GDPR):** Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato ha il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali (Piazza Venezia n. 11 - 00187 Roma - protocollo@pec.gpdp.it), qualora ritenga che il trattamento che lo riguarda violi il GDPR.

Per l'esercizio di tali diritti, l'interessato può contattare il Titolare del trattamento o il Responsabile della Protezione dei Dati (RPD/DPO) ai recapiti indicati al punto 3 della presente informativa.

9. Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

Il Comune di Arvier ha condotto, o si impegna a condurre, una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi dell'articolo 35 del GDPR, in quanto il trattamento di dati personali tramite videosorveglianza costituisce un'attività che, per sua natura, ambito di applicazione e finalità, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La DPIA analizza i rischi e le misure per mitigarli, garantendo che il trattamento sia conforme ai principi del GDPR.

10. Trasferimento di Dati a Paesi Terzi o Organizzazioni Internazionali

Non è previsto il trasferimento di dati personali raccolti tramite il sistema di videosorveglianza a Paesi terzi al di fuori dell'Unione Europea o dello Spazio Economico Europeo, né ad organizzazioni internazionali.

[Luogo], [Data]

Il Titolare del Trattamento Il Sindaco del Comune di Arvier

---

16. Conservazione e scarto dei documenti

Il Titolare del trattamento, in qualità di soggetto pubblico, è tenuto ad applicare le disposizioni in materia di gestione documentale e conservazione dei documenti amministrativi, nel rispetto della normativa vigente. In particolare, l'Ente adotta il **Massimario di selezione e scarto** pubblicato dall'**AgID** (Agenzia per l'Italia Digitale), quale strumento ufficiale per la classificazione, la valutazione e la determinazione dei tempi di conservazione o eventuale scarto dei documenti informatici.

Tale massimario rappresenta un riferimento normativo e operativo fondamentale per garantire la corretta conservazione dei fascicoli digitali, la razionalizzazione degli archivi e il rispetto dei tempi di tenuta previsti dalla normativa archivistica e amministrativa. La sua applicazione consente di definire, per ciascuna tipologia documentale, **la durata minima di conservazione**, **le modalità di scarto** e **le eventuali esigenze di conservazione permanente**, anche ai fini della tutela giuridica, amministrativa e storica degli atti.

I fascicoli e i documenti digitali prodotti o acquisiti dall'Ente sono conservati all'interno di una **piattaforma di conservazione a norma**, così come previsto dall'**art. 44 del Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005)**. Tale conservazione è finalizzata a garantire nel tempo l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti informatici. Il sistema di conservazione, conforme alle Linee Guida AgID, deve essere gestito internamente o affidato a un conservatore accreditato, mediante apposito contratto e nomina a responsabile esterno del trattamento, se previsto.

I tempi di conservazione sono definiti, oltre che dal Massimario AgID, anche sulla base di quanto disposto dal **D.P.R. 445/2000**, che disciplina la formazione, gestione e conservazione della documentazione amministrativa, nonché da eventuali altre disposizioni normative settoriali applicabili in relazione alla tipologia degli atti trattati (es. normativa fiscale, contabile, contrattuale, ecc.).

17. Whistleblowing

In ottemperanza a quanto previsto dalla Direttiva (UE) 2019/1937 e dal D.Lgs. 10 marzo 2023, n. 24, si precisa che, alla data di redazione del presente MOP, il **Comune di Arvier** ha provveduto alla creazione e al mantenimento di un canale interno per le segnalazioni di illeciti (whistleblowing).

18. Checklist degli adempimenti

GOVERNANCE E ORGANIZZAZIONE

Nome Adempimento	Data Adozione	Scadenza/Revisione/ Ultimo aggiornamento	NOTE
Nomina DPO (Data Protection Officer)	Decreto n.1/2023	31/12/2026	I&P Partners Srl, Dott. Ivano Pecis
Registro dei Trattamenti (art. 30 GDPR)	25/05/2018		
Nomine Responsabili Esterni (contratti art. 28 GDPR)	Guarda par. 4.2		
Nomine Autorizzati al trattamento	Guarda par. 3.1		

Nome Adempimento	Data Adozione	Scadenza/Revisione/ Ultimo aggiornamento	NOTE
Registro delle misure di sicurezza tecniche e organizzative			
Esecuzione DPIA per trattamenti ad alto rischio			
Whistleblowing (Regolamento+informativa+DPIA)			

INFORMATIVE E CONSENSI

Nome Adempimento	Data Adozione	Ultimo aggiornamento	Note
Informative Privacy clienti/utenti (art. 13 GDPR)			
Informative Privacy dipendenti/collaboratori			
Informative Privacy fornitori/partner			
Moduli acquisizione consensi (marketing, profilazione)			
Cookie Policy e Banner consensi sito web	Guarda par. 12	Guarda par. 12	
Informative per sistemi videosorveglianza			

DATA BREACH E GESTIONE INCIDENTI

Nome Adempimento	Data Adozione	Ultimo aggiornamento	Note
Procedura gestione Data Breach			
Modello comunicazione Data Breach agli interessati			
Registro violazioni dati personali			

GESTIONE DIRITTI INTERESSATI

Nome adempimento	Ultimo aggiornamento	Note

Modulistica da trasmettere		
Registro richieste interessati		

FORMAZIONE E CONSAPEVOLEZZA

Nome Adempimento	Data	Ultimo aggiornamento	Note
Formazione GDPR generale			
Formazione specialistica ruoli chiave (IT, HR, Marketing)			
Registro formazioni			
Test valutazione conoscenze privacy			
Campagne di awareness interna			

CONSERVAZIONE E CANCELLAZIONE DATI

Nome Adempimento	Data Adozione	Ultimo aggiornamento	Note
Policy di retention per categorie di dati			
Procedure di cancellazione/anonimizzazione			
Sistema automatico di scadenza dati			
Procedura archiviazione documentale			
Registro cancellazioni effettuate			

AUDIT E CONTROLLI PERIODICI

Data	Oggetto