REGOLAMENTO PER SISTEMA DI VIDEOSORVEGLIANZA DELLE SEDI

DI

AMI S.P.A.- AZIENDA PER LA MOBILITA' INTEGRATA E TRASPORTI con sede legale in URBINO (PU)

PIAZZALE ELISABETTA GONZAGA 15 CAP 61029, CF/PI 01482560412

Sommario

Oggetto

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di impianti di videosorveglianza nelle aree di competenza di Ami SpA, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle Persone fisiche, con particolare riferimento alla riservatezza e all'identità personale e garantisce i diritti delle persone coinvolte nel trattamento dei dati.

   Gli impianti sono presenti nelle seguenti sedi

   Biglietteria P.le Falcone e Borsellino a Pesaro (PU)

   Deposito e uffici Via dei Canonici, Pesaro (PU)

   Deposito Via I Maggetti Urbino (PU)

   Biglietteria Via Carlo Pisacane 1 Fano (PU)

   (Si allega Planimetria con il posizionamento delle telecamere)

2. Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal Regolamento UE 2016/679, dal D. Lgs 30 giugno 2003, n. 196 aggiornato al D. Lgs 101/2018, e dalla normativa vigente applicabile in materia di videosorveglianza.

Normativa di riferimento

- Art. 4 della legge 20 maggio 1970 n. 300 "Statuto dei lavoratori", così come modificato dall'art. 23 del D.Lgs. 14/09/2015 n°151, Jobs Act, del 2015, secondo il quale "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro […]";
- il Regolamento Europeo 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- il "Provvedimento in materia di videosorveglianza", pubblicato in G.U. n°99 del 29/04/2010, nel quale il Garante per la protezione dei dati personali ha dettato una serie di regole in materia;
- le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video;
- D. Lgs 104/2022 (c.d. Decreto Trasparenza) "Attuazione della direttiva UE 2019/1152 del Parlamento Europeo e del Consiglio del 20 giugno 2019, relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione Europea
- nota n. 2572 del 14 aprile 2023 dell'Ispettorato Nazionale del Lavoro;
- i provvedimenti e la normativa specifica in materia.

Definizioni

1. Ai fini delle definizioni di cui al presente Regolamento si deve fare riferimento all'art. 4 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Ai fini del presente regolamento si intende:

   a. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
   b. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
   c. «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
   d. «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
   e. «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
   f. «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;
   g. «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
   h. «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
   i. «violazione dei dati personali»: 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;
   j. «comunicazione», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

k. «diffusione» il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

l. «dato anonimo», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

m. «blocco», la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

Principi generali

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali ai sensi dell'art. 4 del Regolamento Europeo. Il suddetto trattamento si fonda sui principi di liceità, necessità, proporzionalità e finalità, come di seguito definiti:

- Principio di liceità: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza è effettuato per garantire maggior tutela dei lavoratori, degli utenti e dell'azienda (tutela del patrimonio aziendale);
- Principio di necessità: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità;
- Principio di proporzionalità: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento;
- Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi, è consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

Finalità dell'impianto di videosorveglianza.

La finalità dell'utilizzo degli impianti di videosorveglianza è quella di garantire la tutela del patrimonio aziendale (e quindi al controllo di furti, atti vandalici o accessi di terze persone non autorizzate e per la conservazione di elementi di prova (EDPB guidelines 2019), adottando misure idonee a prevenire, impedire e comunque ostacolare atti criminosi nei confronti del patrimonio aziendale e dei lavoratori e a tutela della clientela.

Le basi legittime di suddette finalità sono il perseguimento di un legittimo interesse del titolare del trattamento o di terzi (Art. 6 par. 1 lett. f) del GDPR), l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (Art. 6, comma 1, lett. e) e l'adempimento di obblighi di legge ai quali è soggetto il titolare del trattamento (Art. 6 par. 1 lett. c) del GDPR).

L'attività di videosorveglianza e di registrazione delle immagini rilevate non è utilizzata per fini diversi da quelli esplicitati.

Titolare del Trattamento

AMI S.P.A.- AZIENDA PER LA MOBILITA' INTEGRATA E TRASPORTI con sede legale in URBINO (PU) PIAZZALE ELISABETTA GONZAGA 15 CAP 61029, CF/PI 01482560412 è il titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza**.** Al Titolare del trattamento compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza dello stesso. Il titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza:

a. definisce le linee organizzative per l'applicazione della normativa di settore;

b. effettua le notificazioni al Garante per la protezione dei dati personali;

c. nomina i responsabili dei dati trattati acquisiti mediante l'utilizzo degli impianti di videosorveglianza, impartendo istruzioni ed assegnando compiti e responsabilità;

d. detta le linee guida di carattere fisico, logico ed organizzativo per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;

e. vigila sulla puntuale osservanza delle disposizioni impartite

Il Titolare può essere contattato alla mail info@amispa.postacert.it o a mezzo posta all'indirizzo sopra indicato. Per maggiori informazioni circa il trattamento dei dati personali effettuato attraverso tale sistema, è possibile contattare il DPO al seguente recapito *dpo@amibus.it*.

Soggetti esterni autorizzati al trattamento dei dati ricavati dal Sistema di Videosorveglianza

Il Titolare può ricorrere a Soggetti esterni che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate che assicurino la tutela dei diritti dell'interessato. Il titolare procede a designare con atto scritto il Responsabile dei dati trattati e, quest'ultimo provvede ad individuare, sempre in forma scritta, le persone fisiche autorizzate al trattamento. Il Titolare ed il Responsabile dei dati trattati vigilano sulla condotta tenuta da chiunque agisca sotto la loro autorità e abbia accesso ai dati personali; provvedono altresì ad istruire e formare i soggetti autorizzati sulle finalità e sulle modalità del trattamento, sul corretto utilizzo delle procedure di accesso ai sistemi, sugli obblighi di custodia dei dati e, più in generale, su tutti gli aspetti aventi incidenza sui diritti dei soggetti interesse.
A tal fine il Titolare ha formalmente incaricato una società di vigilanza privata al trattamento dei dati personali, sia alla visualizzazione in tempo reale in caso di allarme e sia alla conservazione delle immagini per 72 ore. La società di vigilanza privata individuata per il servizio è la Vigilar Srl, con sede in Via dell'Abbazia 1/A a Fano (PU). Vigilar Srl è stata formalmente nominata Responsabile del Trattamento e opera sulla base di istruzioni precise (ex art. 28 del RGPD). Il Responsabile del trattamento dovrà:

- individuare e nominare con propri atti i soggetti autorizzati al trattamento impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29, RGPD; detti soggetti saranno opportunamente istruiti e formati da parte del Responsabile del trattamento con riferimento alla tutela del diritto alla riservatezza nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati;
- verificare e controllare che il trattamento dei dati effettuato mediante sistema di videosorveglianza, sia realizzato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicura che i dati personali siano trattati in modo lecito, corretto e trasparente; garantisce altresì che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;

- assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, adottare tutte le misure tecniche ed organizzative necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;
- assistere il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del Regolamento Europeo;
- assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti del Titolare;
- garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, è responsabile della formale e tempestiva formulazione della proposta di adozione delle misure necessarie nei confronti del Titolare;
- assicurare l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;
- assistere il Titolare nelle eventuali procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del GDPR;
- assistere il Titolare nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR e del precedente art. 6 del presente Regolamento e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del GDPR;
- il Responsabile affianca il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1, del GDPR, nell'istituzione e aggiornamento del Registro delle attività di trattamento, tenuto in forma scritta, anche in formato elettronico;
- garantire che il Responsabile della Protezione dei Dati designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e si impegna ad assicurargli l'affiancamento necessario per l'esecuzione dei suoi compiti;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;
- rendersi responsabile della custodia e del controllo dei dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- assicurare che i soggetti autorizzati si attengano, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantisce che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;
- garantire la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale autorizzato con riferimento ai trattamenti realizzati mediante l'impianto d videosorveglianza dell'Ente, previo consulto del

Responsabile della Protezione dei dati, necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

- vigilare sul rispetto da parte dei soggetti autorizzati degli obblighi di corretta e lecita acquisizione dei dati e di utilizzazione degli stessi.

Accesso ai sistemi

L'accesso alle immagini raccolte attraverso i sistemi di videosorveglianza di cui al presente regolamento avviene esclusivamente da parte del Responsabile esterno per tramite dei suoi incaricati. Un file di log, generato automaticamente dal sistema informatico, consente di registrare gli accessi logici effettuati dai singoli operatori, le operazioni dagli stessi compiute sulle immagini registrate ed i relativi riferimenti temporali. Tale file non è soggetto a cancellazione e sarà conservato per un periodo di tempo non inferiore a 6 mesi.

- **Accesso ed estrazione dei dati**. Le operazioni di accesso ed estrazione dei dati raccolti è delegato al Responsabile Esterno, solo su preventiva autorizzazione del Titolare. Le operazioni in oggetto sono monitorate tramite il sistema di log e tracciatura fornite dal sistema. È consentita l'estrazione di copia dei dati acquisiti, nonché il riversamento su supporto digitale, nei casi previsti dalla legge, ai fini della difesa di un diritto o su specifica richiesta investigativa dell'autorità giudiziaria. È fatta quindi salva la comunicazione dei dati richiesti, in conformità della legge, da Forze di Polizia, dell'autorità giudiziaria, da organismi di sicurezza e altri enti per finalità di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati. Le registrazioni estratte devono avere requisiti tali da garantirne l'accesso esclusivamente a soggetti preventivamente autorizzati. I supporti digitali su cui vengono riversati i dati devono essere custoditi in sicurezza. Il Titolare ha provveduto a disciplinare le modalità di richiesta di accesso e di estrazione dei dati. Non sono previste altre modalità di richiesta al di fuori della procedura identificata dal Titolare.

- **Ambito di comunicazione dei dati**. L'estrazione e la comunicazione di cui sopra saranno effettuate dal Responsabile Esterno ai soggetti e per le finalità sopra individuate. Tutte le comunicazioni effettuate devono essere annotate in un registro ad accesso riservato conservato presso il Comando.

- **Gestione delle dotazioni tecnologiche**. Le telecamere possono essere sottoposte ad interventi di carattere manutentivo da parte del Responsabile del trattamento (ex art. 28 del RGPD) e da soggetti terzi appositamente individuati e autorizzati. A tal fine i tecnici installatori e manutentori del sistema ed il personale tecnico informatico potranno avere accesso ai sistemi per garantirne il corretto funzionamento ed effettuare attività di manutenzione ordinaria e straordinaria.

- **Diritti e doveri dei soggetti coinvolti.** Tutto il personale coinvolto nel processo di acquisizione, riversamento, estrazione, registrazione e comunicazione dei dati deve essere specificamente autorizzato ed opportunamente istruito all'utilizzo degli strumenti in dotazione. Tutte le attività descritte al punto precedente comportano inevitabilmente anche il trattamento dei dati del personale operante; quindi, questo dovrà essere adeguatamente informato ai sensi di legge. Tali dispositivi non potranno essere utilizzati per esercitare alcun tipo di controllo a distanza sui dipendenti.

Modalità di raccolta e requisiti dei dati personali

I dati personali, nel rispetto dei Principi generali previsti dall'Art. 5 del GDPR, sono

a. trattati in modo lecito, corretto e trasparente;
b. raccolti e registrati per le finalità di cui al precedente art. 1 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi; esatti e, se necessario, aggiornati;
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti e/o trattati;
d. esatti e, se necessario, aggiornati. Saranno adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
e. conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo comma 3;
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. La sicurezza dei dati personali si intende per tutto il trattamento.

Obblighi degli operatori

L'utilizzo delle telecamere è consentito solo per le finalità sopra dichiarate. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui sopra e a seguito di regolare autorizzazione di volta in volta richiesta al Titolare.

Informazioni da fornire al momento della raccolta

Ami SpA, in ottemperanza a quanto disposto dall'art. 13 del Regolamento Europeo 679/2016 "Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato"", si obbliga ad affiggere un'adeguata segnaletica permanente, in corrispondenza dell'area di ripresa delle telecamere e comunque all'ingresso delle aree videosorvegliate, con l'apposizione di cartelli segnaletici, su cui sono riportate le informazioni previste dalla norma, tra cui il Titolare del Trattamento e i contatti, la finalità dello stesso, i tempi di conservazione, sulla base di quanto raffigurato all'allegato 1.

Dette segnalazioni rispettano le indicazioni fornite dal Garante della Privacy e dall'European Data Protection Board – EDPB (***Linee Guida 3/2019***). Sul sito istituzionale del Titolare www.amibus.it è pubblicata l'informativa contenente le modalità e le finalità per cui gli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Diritti dell'interessato

In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:

- di conoscere l'esistenza di un trattamento di dati che possono riguardarlo;
- di essere informato sugli estremi identificativi del titolare, del responsabile e degli incaricati, oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;

- di ottenere, a cura dell'incaricato, senza ritardo e in tempi adeguati, nel rispetto delle normative vigenti:
  i. la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;
  ii. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
  iii. la possibilità di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Per ciascuna delle richieste di cui sopra, può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente. I diritti di cui al presente articolo, se riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
Nell'esercizio dei propri diritti l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

Le istanze di cui al presente articolo possono essere trasmesse al titolare utilizzando il modello in allegato e inviandolo, secondo le modalità previste, a *info@amispa.postecert.it* o all'attenzione del DPO alla mail *dpo@amibus.it*. Deve essere da subito evidente l'oggetto della comunicazione che dovrà specificare_*RICHIESTA DEI DIRITTI DI CUI AGLI ARTT. 15/22 DEL GDPR.*
Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Accesso alle immagini

L'accesso alle immagini e quindi alle registrazioni può essere richiesto dall'interessato solo nel caso siano presenti dati che lo riguardano. Non è possibile richiedere immagini nel quale siano presenti soggetti diversi dall'interessato se non previa denuncia all'Autorità e alla Polizia Postale. Le eventuali immagini e/o informazioni che possano rendere identificabile un soggetto terzo saranno oscurate.
Si raccomanda nel caso si intenda richiedere l'accesso alle immagini, di inviare preventiva comunicazione al Titolare attraverso i canali comunicati per il BLOCCO DELLE IMMAGINI, che consentirà di salvare le stesse dalla cancellazione automatica che avviene trascorso il tempo di 72 ore. Il blocco consentirà di "congelare" le immagini per un tempo non superiore ai 7 giorni, in modalità sicura con misure tecniche specifiche. Allo scadere di tale termine le immagini verranno cancellate in maniera irreversibile.
Il Blocco delle immagini avverrà da parte del Responsabile Esterno che provvederà ad "archiviare" la parte di immagini richiesta. L'istanza va trasmessa al titolare utilizzando il modello in allegato e inviandolo a *info@amispa.postecert.it* o all'attenzione del DPO alla mail *dpo@amibus.it*. È obbligatorio utilizzare il modello in allegato compilato in ogni parte per consentire al titolare di poter ottemperare alla richiesta. Eventuali carenze nelle informazioni potrebbero non consentire al Titolare di poter gestire la richiesta.

La comunicazione inviata nelle modalità previste dovrà contenere nell'oggetto la dicitura *"RICHIESTA DEI DIRITTI DI CUI AGLI ARTT. 15/22 DEL GDPR _ACCESSO/BLOCCO VIDEOREGISTRAZIONI".*

Sicurezza dei dati

I dati raccolti mediante il sistema di videosorveglianza dovranno essere protetti con idonee e preventive misure tecniche e organizzative in grado di garantire un livello di sicurezza adeguato al rischio. Dette misure, in particolare, assicurano:

a. la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

b. il ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico;

c. la sistematica e periodica verifica e valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ai sensi dell'art. 32, Paragrafo 2, RGPD, nel valutare l'adeguato livello di sicurezza, il Titolare terrà conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati dal titolare.

Accesso agli impianti e ai dati

L'accesso agli impianti di videosorveglianza di cui al presente regolamento avviene dalla centrale operativa della società di vigilanza privata a ciò autorizzata. L'accesso ai dati può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate dal responsabile del trattamento. L'accesso ai dati registrati al fine del loro riesame, nel rigoroso arco temporale previsto per la conservazione, è consentito solamente in caso di effettiva necessità per il conseguimento delle finalità specificate nel presente Regolamento.

1. L'accesso alle immagini è consentito esclusivamente:

   a. al Titolare del Trattamento per le finalità di cui sopra;

   b. alle Forze di Polizia (sulla base di richiesta scritta formulata dal rispettivo comando di appartenenza e acquisita dall'Ente) nonché per finalità di indagine dell'Autorità Giudiziaria (sulla base di formale richiesta proveniente dal Pubblico Ministero e acquisita dall'Ente);

   c. alla società di vigilanza privata nei limiti strettamente necessari all'accordo in essere con il Titolare;

   d. all'interessato del trattamento (in quanto oggetto delle riprese) che abbia presentato istanza di accesso alle immagini, previo accoglimento della relativa richiesta. L'accesso da parte dell'interessato sarà limitato alle sole immagini che lo riguardano direttamente; al fine di evitare l'accesso ad immagini riguardanti altri soggetti, dovrà pertanto essere utilizzata, da parte de soggetto incaricato, una schermatura del video ovvero altro accorgimento tecnico in grado di oscurare i riferimenti a dati identificativi delle altre persone fisiche

Allegati:

1) informativa breve;

2) informativa completa;

3) modello per accesso/blocco videoregistrazioni dell'impianto di videosorveglianza

Allegato 01


AREA VIDEOSORVEGLIATA
L'informativa completa sul trattamento dei dati è disponibile su www.amibus.it
LA REGISTRAZIONE È EFFETTUATA DA AMI SPA. L'IMPIANTO E' COLLEGATO CON UNA SOCIETA' DI VIGILANZA PRIVATA
LE IMMAGINI SARANNO CONSERVATE PER UN PERIODO DI 72 ORE
FINALITÀ DELLA VIDEOSORVEGLIANZA: TUTELA DEL PATRIMONIO AZIENDALE
È POSSIBILE ACCEDERE AI PROPRI DATI ED ESERCITARE GLI ALTRI DIRITTI RICONOSCIUTI DALLA LEGGE RIVOLGENDOSI AL TITOLARE DEL TRATTAMENTO (0722/376711)
È POSSIBILE CONTATTARE IL RESPONSABILE DELLA PROTEZIONE DEI DATI ALLA MAIL DPO@AMIBUS.IT

Allegato 02

INFORMATIVA PER SISTEMA DI VIDEOSORVEGLIANZA SEDI

Installazione impianto di telecamere per videosorveglianza con registrazione delle immagini (informativa sulla base del Regolamento Europeo 679/2016, Provvedimento in materia di videosorveglianza 8 aprile 2010 e Circolare 5/2018 dell'INL)

Ai sensi degli Art. 13/14 del Regolamento Europeo 679/2016 relativo alla protezione ed al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale della protezione dei dati), si informa che all'interno delle sedi sotto riportate è attivo un sistema di videosorveglianza:

Biglietteria P.le Falcone e Borsellino a Pesaro (PU)

Deposito e uffici Via dei Canonici, Pesaro (PU)

Deposito Via I Maggetti Urbino (PU)

Biglietteria Via Carlo Pisacane 1 Fano (PU)

TITOLARE DEL TRATTAMENTO E LUOGO DI TRATTAMENTO DEI DATI

Il trattamento dei dati ha luogo presso la predetta sede del titolare e presso i soggetti terzi individuati. Potete contattare il Titolare del Trattamento alla mail info@amispa.postecert.it o a mezzo posta all'indirizzo della sede legale: P.le E. Gonzaga, 15 – 61029 Urbino (PU)

RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

In ragione delle attività di trattamento svolte all'interno della società, il Titolare del trattamento ha designato, ai sensi dell'art. 37 del Regolamento Europeo, un Responsabile della Protezione dei dati (Data Protection Officer_DPO). Il DPO può essere contattato alla mail dpo@amibus.it

FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO

La finalità dell'utilizzo degli impianti di videosorveglianza è quella di garantire la tutela del patrimonio aziendale (e quindi al controllo di furti, atti vandalici o accessi di terze persone non autorizzate e per la conservazione di elementi di prova (EDPB guidelines 2019), adottando misure idonee a prevenire, impedire e comunque ostacolare atti criminosi nei confronti del patrimonio aziendale e dei lavoratori e a tutela della clientela.

Le basi legittime di suddette finalità sono il perseguimento di un legittimo interesse del titolare del trattamento o di terzi (Art. 6 par. 1 lett. f) del GDPR), l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (Art. 6, comma 1, lett. e) e l'adempimento di obblighi di legge ai quali è soggetto il titolare del trattamento (Art. 6 par. 1 lett. c) del GDPR).

MODALITÀ DI TRATTAMENTO

La visione delle immagini registrate può avvenire esclusivamente nei seguenti casi:

1. in caso di evento criminoso o che richieda indagini e accertamenti da parte del Titolare. Il Titolare può accedere per esigenze connesse all'assolvimento di norme di legge e/o regolamentari e a garanzia della tutela della clientela e/o del patrimonio aziendale;
2. dopo formale denuncia alle autorità competenti e/o dopo formale richiesta da parte delle Forze dell'Ordine o

dell'autorità giudiziaria competente;

3. a seguito dell'esercizio del diritto di accesso ai dati personali ai sensi dell'art. 15 del GDPR. L'interessato a cui le immagini afferiscono, può richiedere istanza di accesso ai dati, esercitata ai sensi della suddetta normativa, secondo le modalità rese disponibili dall'azienda.

AMBITO DI COMUNICAZIONE

I dati oggetto del trattamento saranno comunicati, solo ed esclusivamente per lo svolgimento delle attività attinenti alle finalità di cui sopra, a terzi autorizzati e/o personale dipendente, in particolare:

- Personale specificatamente autorizzato al trattamento;
- Soggetti che forniscono servizi per la gestione del sistema di videosorveglianza;
- Società di Vigilanza Privata;

I soggetti appartenenti alle categorie suddette hanno presentato garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate e, laddove non identificabili come *Autonomi Titolari del Trattamento*, sono stati nominati *Responsabili del trattamento dei dati* con atto formale e scritto, impegnandosi a trattare i dati solo su istruzioni documentate del Titolare del Trattamento. L'elenco dei responsabili è costantemente aggiornato e disponibile, a richiesta, presso la sede del Titolare del Trattamento.

Ogni ulteriore comunicazione avverrà solo previo esplicito consenso. Il sottoscritto, quale Titolare del Trattamento, ha provveduto a formare il personale autorizzato sulle norme previste dalla disciplina vigente in materia di dati personali.

ATTIVITÀ DI SORVEGLIANZA E DIVIETO DI CONTROLLO

Gli impianti di videosorveglianza sono installati nel rispetto della disciplina in tema di protezione di dati personali e in particolare dello Provvedimento 08 aprile 2010 dell'Autorità Garante per la protezione dei dati personali, dello Statuto dei Lavoratori (L. 300/1970) e delle Linee Guida 3/2019 dell'EDPB. Nelle attività di sorveglianza sarà quindi rispettato il divieto di controllo a distanza dell'attività lavorativa e non saranno effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa.

La visualizzazione delle immagini, fatta in maniera non sistematica ma solo ove intervengono situazione che richiedono accertamenti e valutazioni più approfondite per le finalità sopra riportate, come ipotesi di atti criminosi, eventi dannosi o possibili situazioni di pericolo, laddove mostri situazioni non conformi alle disposizioni aziendali, non potrà essere da solo causa di provvedimento sanzionatorio ma potrà costituire, laddove ci siano i presupposti oggettivi e fondati di verifica da parte del datore di lavoro, un supporto all'accertamento dell'obbligo di diligenza del lavoratore e dell'eventuale adozione di provvedimenti sanzionatori.

DIRITTI DEGLI INTERESSATI

Gli interessati potranno esercitare i diritti ai sensi del Capo III del Regolamento Europeo 679/2016 utilizzando l'apposito modello e inviandolo, secondo le modalità previste, a *info@amispa.postecert.it* o all'attenzione del DPO alla mail *dpo@amibus.it* . Maggiori informazioni sono disponibili nel sito www.amibus.it.

AMI SpA

Per presa visione, comprensione e accettazione di quanto espresso

_____

Allegato 03

Spett.le AMI SPA
Piazzale E. Gonzaga, 15 - 61029 Urbino (PU)
PEC: *info@amispa.postecert.it*
Alla c.a. del Responsabile della Protezione Dati
Mail: *dpo@amibus.it*

ACCESSO/BLOCCO VIDEOREGISTRAZIONI DELL' IMPIANTO DI VIDEOSORVEGLIANZA

Il/La sottoscritto/a

Cognome _____ Nome _____

Nato/a a _____ il_____/_____/_____ Residente in _____

Prov. (_____) Indirizzo di residenza _____

Telefono/Cellulare _____

E-mail _____PEC _____

PREMETTE

☐ di essere transitato in spazi ripresi dal sistema di videosorveglianza di competenza di AMI SPA

oppure

☐ di avere subito/assistito a quanto più oltre descritto, in spazi che presume essere ripresi dal sistema di videosorveglianza di competenza di AMI SPA (specificare):

_____

_____

_____

- di essere consapevole che le immagini registrate vengono conservate per max 72 ore;
- di essere altresì consapevole che qualora, entro i termini sopra indicati, venga presentata al titolare del sistema di videosorveglianza motivata e dettagliata richiesta di accesso alle videoregistrazioni, per fatti costituenti ipotesi di reato le immagini (ove reperite) possono essere acquisite dall'autorità giudiziaria e/o di polizia a seguito di apposita ufficiale richiesta delle stesse;

☐ che intende esercitare il diritto di accesso, riconosciuto dall'art. 15 del Regolamento UE 679/2016 (GDPR), al seguente scopo:

(a) ☐ accertare se siano state raccolte immagini che riguardano il sottoscritto;

(b) ☐ eventualmente richiedere il blocco delle immagini (non cancellazione) al fine di metterle a disposizione dell'autorità giudiziaria / di polizia (che indaga sui fatti descritti) dietro apposita ufficiale richiesta delle stesse autorità o, nell'ambito delle investigazioni difensive, per consegnarle al difensore della persona sottoposta alle indagini (a norma dell'art. 391-quater c.p.p.) sempre dietro apposita ufficiale;

(c) ☐ Altro:

_____

_____

_____

_____

- di essere consapevole che, se le immagini contengono dati riferibili a terzi, l'accesso del sottoscritto è consentito nei limiti stabiliti dalla vigente normativa, e dunque soltanto se "la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi" a detti terzi, e conseguentemente di accettare:

  - in relazione allo scopo sopra indicato sub (a), che gli eventuali dati riferiti a terze persone vengano resi incomprensibili;
  - in relazione allo scopo sopra indicato sub (b), che le immagini, conservate e lasciate integre, vengano consegnate direttamente ai soggetti specificati sopra indicato sub (b).

Tutto ciò premesso il sottoscritto, a norma dell'art. 15 del GDPR

CHIEDE

di esercitare il diritto di accesso alle immagini rilevate da apparati di videosorveglianza di AMI SpA, che potrebbero aver registrato dati personali a sé stesso afferenti.

Per permettere di individuare tali immagini, forniscono le seguenti informazioni:

1. luogo o luoghi di possibile ripresa:

_____

_____

_____

2. data di possibile ripresa: _____

3. fascia oraria di possibile ripresa (approssimazione di 30 minuti) dalle ore _____ alle ore _____

4. abbigliamento e/ accessori al momento della possibile ripresa:

_____

_____

_____

7. attività svolta durante la ripresa:

_____

_____

_____

8. altri elementi atti a facilitare l'individuazione del sottoscritto:

_____

_____

ALLEGA

fotocopia di un documento di identità in corso di validità del dichiarante anche in caso di trasmissione dell'istanza a mezzo posta elettronica certificata. Il documento non va trasmesso unicamente se la richiesta è sottoscritta con firma digitale o con altro tipo di firma elettronica qualificata o con firma elettronica avanzata (art. 65, c. 1, lett. a), del d.lgs. n. 82/2005).

Informativa sul trattamento dei dati personali forniti con l'istanza (ai sensi dell'art. 13 del Regolamento UE 2016/679)

Il/La sottoscritto/a è consapevole che i dati personali contenuti nella presente istanza sono oggetto di trattamento informatico e/o manuale e potranno essere utilizzati esclusivamente per gli adempimenti di legge. I dati saranno trattati dal Titolare nel rispetto delle disposizioni del Regolamento UE 2016/679 con le modalità previste dall'informativa completa pubblicata sul sito *web* istituzionale (www.amibus.it).

Luogo e data

_____

Firma del/la richiedente

_____

(firma per esteso e leggibile)