REGOLAMENTO
PER L'INSTALLAZIONE E L'UTILIZZO DI IMPIANTI
DI VIDEOSORVEGLIANZA

adozione:	Determina dell'Amministratore Delegato del 23 settembre 2024.

Sommario

CAPO I
PRINCIPI GENERALI

ARTICOLO 1 - OGGETTO E NORME DI RIFERIMENTO

1. Il presente regolamento disciplina l'installazione nonché l'utilizzo dei sistemi di videosorveglianza all'interno ed all'esterno dei presidi dell'Azienda Generalfinance S.p.A. (di seguito denominata Azienda).
2. Per tutto quanto non è dettagliatamente disciplinato nel presente documento si rinvia a quanto disposto dal Regolamento (UE) del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati 2016/679 - *General Data Protection Regulation* pubblicato sulla Gazzetta Ufficiale dell'Unione Europea - GUUE il 4 maggio 2016) d'ora in poi GDPR e che abroga la direttiva 95/46/CE, dal Codice in materia di protezione dei dati personali approvato con Decreto Legislativo 30 giugno 2003, n.196 come novellato dal Decreto Legislativo 10 agosto 2018, n.101 e dal Provvedimento del Garante per la protezione dei dati personali in materia di videosorveglianza del 8 aprile 2010.

ARTICOLO 2 - DEFINIZIONI

1. Ai fini del presente Regolamento si intende:

   a. per "**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. per "**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. per "**titolare del trattamento**", L'Azienda Generalfinance S.p.A, nella persona del Legale Rappresentante Massimo Gianolli cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali;

   d. per "**responsabile del trattamento**" ex art. 28 del Regolamento europeo 2016/679, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

   e. per "**amministratore di sistema**", figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e alle quali è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione;

   f. per **"responsabile interno"**, la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento di dati personali al quale il titolare stesso demanda alcune responsabilità previste nel presente regolamento;

   g. per **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare;

   h. per "**interessato**", la persona fisica a cui si riferiscono i dati personali;

   i. per **"profilazione"**, qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

j. per **"pseudonimizzazione"**, il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

k. per **"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;

l. per "**comunicazione**", il dare conoscenza dei dati personali a soggetti determinati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m. per "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n. per "**dato anonimo**", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non possa essere associato ad un interessato identificato o identificabile;

o. per **"limitazione"**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

Per ulteriori definizioni si rinvia a quanto previsto dall'art.4 del Regolamento (UE) 2016/679.

ARTICOLO 3 - FINALITÀ

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza, i cui *monitor* per la visione delle immagini riprese dalle telecamere sono posizionati presso Biella Via Carso e Milano Via Stephenson in locali debitamente realizzati[1].
2. L'Azienda attua un sistema di videosorveglianza finalizzato esclusivamente allo svolgimento delle proprie funzioni istituzionali, ovvero:
   - per garantire la sicurezza del patrimonio aziendale, mobiliare ed immobiliare, e per la protezione delle persone che, a vario titolo, accedono e/o sostano negli ambienti interni alle strutture aziendali;
   - per la tutela della sicurezza e dell'ordine pubblico.

FINALITÀ DI SICUREZZA

Al fine di perseguire le finalità di sicurezza l'Azienda installa sistemi di videosorveglianza esclusivamente presso zone soggette a concreti pericoli o per le quali ricorre un'effettiva esigenza di deterrenza.
Gli impianti di videosorveglianza sono attivati quando altre misure siano ponderatamente valutate insufficienti o inattuabili o risultino inefficaci altri idonei accorgimenti, quali ad esempio: controlli da parte degli addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi ecc.

ARTICOLO 4 - DATI PERSONALI

1. Il trattamento dei dati personali attraverso il sistema di videosorveglianza avviene secondo i principi generali di:
   - responsabilizzazione (*accountability*)
     - nel fornire una garanzia di completa accessibilità alle informazioni che riguardano i cittadini in quanto utenti del servizio (principio di trasparenza);

[1] Si precisa che non esistono installazioni fisse di monitor bordo NVR (network video- recorder - il device che concentra le telecamere per ogni sito), né sale di controllo predisposte a tale scopo. Le immagini riprese dalle telecamere, sono accessibili nei seguenti modi: 1) connettendosi direttamente all'NVR di interesse da pc, tramite IP privato o pubblico, UserID e Password.2) Dall'app iVMS-4500 per iOS o Android tramite cellulare (per le persone autorizzate).3) Dalla Centrale Operativa (di seguito C.O.) dell'attuale fornitore di servizi di sicurezza Axitea. È bene specificare che la visione delle immagini da parte della C.O. viene attivata solo in caso di evento di allarme.

- nella capacità effettiva di rendere conto delle scelte fatte, dei comportamenti, delle azioni attuate e di rispondere alle questioni poste dai portatori di interessi generali (principio della responsività);
- nella capacità effettiva di fare rispettare le norme sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori (principio della conformità);

- protezione dei dati fin dalla progettazione (*privacy by design*) ovvero la necessità di tutelare i dati personali sin dalla fase di sviluppo, progettazione, selezione di un progetto che comporti l'utilizzo di applicazioni, servizi e prodotti per il trattamento di dati personali, creando un sistema che sin dall'inizio dell'attività limiti possibili violazioni dei dati raccolti (articolo 25 comma 1 del GDPR);
- protezione dei dati per impostazione predefinita (*privacy by default*) ovvero la necessità di implementare misure giuridiche, tecniche e organizzative efficaci e adeguate a garantire che siano trattati solo i dati personali necessari per ciascuna finalità specifica del trattamento, con l'impostazione a priori della massima protezione dei dati attraverso il loro minimo trattamento sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione, secondo i principi di necessità e pertinenza (articolo 25 comma 2 del GDPR).

2. L'Azienda in qualità di Titolare del trattamento dei dati personali (di seguito Titolare) definisce autonomamente le modalità, le garanzie e i limiti di trattamento dei dati personali, ed elabora specifici modelli organizzativi che ne garantiscano una costante applicazione e monitoraggio.
3. L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite (limitazione delle finalità), registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando quando non indispensabili immagini dettagliate, ingrandite o dettagli non rilevanti (minimizzazione dei dati e rispetto dei principi di pertinenza e non eccedenza). Il trattamento dei dati personali avviene nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche con particolare riferimento al diritto alla protezione dei dati personali e all'identità personale, e in modo da garantirne un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale anche mediante l'adozione di misure tecniche e organizzative (integrità e riservatezza). La localizzazione delle telecamere e le modalità di ripresa sono quindi stabilite in modo conseguente.
4. Il trattamento di dati personali avviene in modo lecito poiché è necessario per il perseguimento del legittimo interesse del titolare del trattamento e necessario per l'esecuzione di un compito di interesse pubblico, in modo corretto e trasparente nei confronti dei soggetti interessati (liceità).
5. L'uso dei dati personali nell'ambito di cui trattasi non necessita pertanto del consenso degli interessati.
6. Gli impianti di videosorveglianza non possono essere utilizzati, in base all'articolo 4 dello Statuto dei lavoratori (Legge n. 300 del 20 maggio 1970) e successive modificazioni per effettuare controlli sull'attività lavorativa dei dipendenti dell'Azienda o di altri datori di lavoro, pubblici o privati.
7. L'impianto di videosorveglianza non può essere utilizzato per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

ARTICOLO 5 - TEMPI DI CONSERVAZIONE DELLE IMMAGINI E FOTOGRAFIE

1. Le immagini registrate dall'impianto di videosorveglianza possono essere conservate per un periodo di tempo non superiore a quello strettamente necessario al soddisfacimento delle finalità dell'impianto, per le quali esse sono state raccolte o successivamente trattate. La conservazione deve essere limitata a poche ore dalla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

2. In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante, a meno che non derivi da una specifica richiesta dell'Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso.

3. L'Azienda stabilisce di conservare di norma le immagini fino a 24 ore successive alla registrazione. Tale termine può essere derogato a seguito di specifica richiesta da parte dell'Autorità Giudiziaria o delle Forze di Pubblica Sicurezza in relazione a un'attività investigativa in corso.

ARTICOLO 6 - TUTELA DELLA RISERVATEZZA DEI LAVORATORI

In considerazione della necessità di salvaguardia dei dipendenti da forme di controllo sul luogo di lavoro e dell'espresso divieto di utilizzo della videosorveglianza come mezzo per operare un controllo a distanza sull'attività svolta da ciascun lavoratore, l'attività disciplinata dal presente testo viene svolta nel pieno rispetto di tale divieto.

Qualora l'installazione degli impianti venga effettuata in aree nelle quali i dipendenti svolgono la loro prestazione o abitualmente frequentati dagli stessi, la ritrazione e le modalità di trattamento della stessa verrà effettuato nei limiti previsti dalla Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) e, in particolare, di quanto disposto dall'art. 4.

Non verranno in ogni caso installati sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori e non destinati all'attività lavorativa (es. bagni, servizi, spogliatoi, docce, locale armadietti e luoghi ricreativi).

CAPO II
OBBLIGHI E ADEMPIMENTI PER I SOGGETTI GESTORI DEL SISTEMA

ARTICOLO 7 - FIGURE DEL TRATTAMENTO

A. TITOLARE DEL TRATTAMENTO

1. Il Titolare del trattamento dei dati relativi a sistemi di videosorveglianza è Generalfinance S.p.A in persona del proprio Legale Rappresentante.
2. Al Titolare compete ogni decisione in ordine alle finalità ed ai mezzi di trattamento dei dati personali, compresi gli strumenti utilizzati e le misure di sicurezza da adottare.

B. RESPONSABILE INTERNO DEL TRATTAMENTO

1. Il Responsabile interno è individuato, previa nomina da effettuare con atto del Legale Rappresentante, quale Responsabile del trattamento dei dati personali, ai sensi dell'art 2-quaterdecies del D.lgs. 196/2003, (in seguito Responsabile interno) rilevati dal sistema di videosorveglianza. Il Responsabile è scelto con provvedimento motivato tra i soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto del presente Regolamento e delle disposizioni di legge vigenti in materia, con particolare riferimento al profilo relativo alla sicurezza, riservatezza e tutela dei diritti dell'Interessato. I compiti affidati al Responsabile interno devono essere specificati per iscritto, in sede di designazione.
2. Il Responsabile interno ha l'obbligo di attenersi a quanto previsto dalla normativa vigente in tema di trattamento dei dati personali, ivi incluso il profilo della sicurezza, ed alle disposizioni del presente Regolamento.
3. Il Responsabile interno procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni previste dalla normativa vigente sulla *privacy* e delle proprie istruzioni.
4. Il Responsabile interno impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento non autorizzato di dati da parte delle persone abilitate all'accesso per la manutenzione e riparazione degli impianti.

C. INCARICATI DEL TRATTAMENTO

1. Il Titolare designa e nomina per iscritto, con apposita lettera di incarico, gli incaricati, ai sensi dell'art dell'articolo dell'art 2-quaterdecies del D.lgs. 196/2003, in numero sufficiente a garantire la gestione del servizio di videosorveglianza.
2. Gli incaricati sono nominati tra i soggetti che per stato di servizio, specifiche attitudini, esperienza, capacità ed affidabilità forniscono idonea garanzia di riservatezza nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
3. Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del Titolare e del Responsabile interno, utilizzando gli impianti nei casi in cui sia indispensabile per gli scopi perseguiti.
4. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente Regolamento.
5. Il Responsabile interno anche con l'eventuale supporto degli incaricati, ha l'obbligo di verificare che le operazioni di utilizzo e trattamento dei dati siano svolte nel rispetto delle norme ed esclusivamente per gli scopi descritti sopra nonché il dovere di impedire che gli stessi siano divulgati a soggetti estranei all'attività di trattamento, salvi i casi d'intervento e/o richiesta da parte degli organi di Autorità Giudiziaria.
6. Il Responsabile interno per la videosorveglianza, unitamente agli Incaricati e a personale autorizzato dal Responsabile interno, tra cui l'amministratore di sistema, sono gli unici ad accedere ai locali in cui sono situate le postazioni di controllo dei sistemi, ad utilizzare gli stessi, a prendere visione ed eventualmente trattare le immagini quando ciò sia necessario per perseguire le finalità indicate nel presente Regolamento.

D. RESPONSABILE ESTERNO EX ART 28 REGOLAMENTO EUROPEO 679/2016

1. Le società (Axitea) incaricate dall'Azienda di effettuare la realizzazione degli interventi di manutenzione ordinaria e straordinaria *hardware* e *software*, comprensiva degli interventi necessari su dispositivi e *software* di archiviazione e di gestione del sistema di videosorveglianza, sono nominate dal Titolare quali Responsabili esterni del trattamento dei dati con apposito atto scritto ai sensi dell'art 28 Regolamento Europeo 679/2016.
2. I rapporti con i responsabili esterni, ex art 28 Regolamento Europeo 679/2016, sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli stati membri.
3. Gli addetti del Responsabile esterno hanno l'obbligo al segreto sulle immagini che eventualmente dovessero visionare nell'esercizio del loro lavoro.

ARTICOLO 8 - OBBLIGHI DEGLI OPERATORI

1. Il settore di ripresa delle telecamere deve essere impostato in modo tale da consentire il controllo e la registrazione di quanto accada nei luoghi pubblici o aperti al pubblico, con esclusione delle proprietà private.
2. 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 all'articolo 3 del presente Regolamento.
3. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.
4. Quale ulteriore misura di sicurezza, al fine di prevenire utilizzi impropri dei filmati, il Titolare e il Responsabile interno sono abilitati ad una verifica periodica (trimestrale) degli accessi al registrato da parte del personale autorizzato; si tratta del mero download dei log (condiviso in un report con l'Ufficio Compliance), senza analisi di dettaglio salvo espresse richieste specifiche da parte della Direzione, dell'Ufficio Compliance, del DPO, o enti quali le forze dell'ordine.

CAPO III
IMPIANTO DI VIDEOSORVEGLIANZA

ARTICOLO 9 - CARATTERISTICHE TECNICHE DELL'IMPIANTO DI VIDEOSORVEGLIANZA E UBICAZIONE

1. Le telecamere posizionate per garantire la sicurezza del patrimonio aziendale, mobiliare e immobiliare, e per la protezione delle persone sono posizionate in punti nevralgici come descritto nell'Allegato 1A. Tale impianto potrà essere eventualmente ampliato secondo gli sviluppi futuri del sistema. Le caratteristiche tecniche dell'impianto sono descritte nell'Allegato 1A.
2. L'utilizzo delle immagini riprese tramite impianti di videosorveglianza è regolata in modo da riguardare solo i dati strettamente necessari alle finalità perseguite.
3. L'installazione degli impianti o la modifica degli stessi è autorizzata dal Titolare del trattamento.
4. Una volta installato e/o modificato l'impianto e prima della messa in funzione dello stesso, il Titolare (o il Responsabile per la videosorveglianza) verifica il rispetto della normativa sulla privacy. Anche nel corso delle registrazioni il Titolare o il Responsabile è legittimato ad effettuare dei controlli al fine di verificare la legittimità delle modalità di registrazione.
5. Gli impianti di videosorveglianza devono:
   a) garantire la necessaria continuità operativa della ripresa;
   b) essere mantenuti in buone condizioni;
   c) essere protetti da possibili atti di vandalismo;
   d) consentire se previsto la registrazione delle immagini;
   e) consentire la cancellazione delle immagini.
6. I locali dove risiedono i dispositivi che governano il funzionamento e l'accesso alle immagini sono protetti da sistemi di controllo accessi. L'accesso a tali locali è consentito soltanto al personale dell'Ufficio Sistemi ICT di Generalfinance, e ad alcuni fornitori strategici. I dispositivi tecnici, sono ubicati nei due CED di Biella e Milano, sotto controllo accessi. I device sono conservati nel rack dove risiedono anche gli altri apparati di rete.

CAPO IV
TRATTAMENTO DEI DATI PERSONALI

ARTICOLO 10 - MODALITÀ DI RACCOLTA E REQUISITI DEI DATI PERSONALI

1. I dati personali oggetto di trattamento vengono:
   a) trattati in modo lecito e secondo correttezza per le finalità di cui all'articolo 3 del presente Regolamento;
   b) trattati in modo pertinente, completo e non eccedente, rispetto alle finalità per le quali sono raccolti o successivamente trattati;
   c) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, con modalità rivolte a salvaguardare l'anonimato anche successivamente alla fase della raccolta, atteso che tali immagini registrate potrebbero contenere dati di carattere personale.
2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza installate consentendo un significativo grado di precisione e di dettaglio della ripresa per le finalità richiamate nel presente regolamento. Le telecamere sono posizionate in punti nevralgici come descritto negli Allegati 1A.
3. Il Titolare si obbliga a non effettuare delle riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato; si tratta di riprese a campo allargato.
4. Il sistema impiegato è programmato in modo da operare, al momento prefissato, per l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In particolare, il periodo di retention delle immagini si attesta sulle 24h previste secondo normativa, dopo le quali queste sono cancellate con procedimento di sovrascrittura locale. Tale funzione viene eseguita con gli strumenti disponibili presenti sull'NVR installato; pertanto, la garanzia della loro non riutilizzabilità è insita nel modo in cui il vendor (Hikvision) ha progettato e costruito l'NVR.

ARTICOLO 11 - ACCERTAMENTI DI ILLECITI ED INDAGINI GIUDIZIARIE O DI POLIZIA

1. In caso di rilevazioni di immagini di fatti concernenti ipotesi di reato o di eventi rilevanti ai fini della pubblica sicurezza, o del patrimonio aziendale, l'incaricato o il Responsabile interno provvede a darne comunicazione senza ritardo all'Autorità competente, provvedendo, nel contempo, alla conservazione delle immagini su appositi supporti.
2. Alle immagini raccolte ai sensi del presente articolo possono accedere, per l'espletamento delle relative indagini, solo gli appartenenti all'Amministrazione Giudiziaria, le persone da essi espressamente autorizzate e gli organi di Polizia.
3. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino una copia delle riprese effettuate, devono presentare un'istanza scritta e motivata indirizzata al Titolare, salvo non sia in essere apposita convenzione.

ARTICOLO 12 - INFORMAZIONI RESE AL MOMENTO DELLA RACCOLTA

1. Tutti coloro che accedono ai locali dell'Azienda devono essere messi in condizione di conoscere la circostanza di poter essere ripresi ed essere informati dell'esistenza di impianti di videosorveglianza.
2. L'Azienda affigge una adeguata segnaletica (cartello) su cui devono essere riportate le informazioni riguardanti il Titolare del trattamento e le finalità perseguite (informativa breve o minima come da Provvedimento in materia di videosorveglianza del 8 aprile 2010 emanato dal Garante per la protezione dei dati personali). L'informativa completa conforme agli articoli 13 e 14 del GDPR è consultabile e reperibile presso i locali aziendali alla reception di entrambe le sedi e nella sezione privacy del sito Generalfinance.
3. Il cartello deve avere un formato ed un posizionamento tali da essere chiaramente visibile all'utenza e deve altresì inglobare il simbolo della telecamera.

ARTICOLO 13 - SICUREZZA DEI DATI

1. I dati sono protetti da misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio di distruzione, di perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati personali.
2. In ossequio al disposto di cui all'art. 35, Paragrafo 3, lett. c), GDPR, poiché il trattamento di dati realizzato mediante il sistema di videosorveglianza dà luogo ad una sorveglianza sistematica su larga scala di una zona accessibile al pubblico, il Titolare procede ad una valutazione di impatto sulla protezione dei dati personali (DPIA). Qualsiasi implementazione e/o modifica dell'impianto dovrà essere preceduta da nuova valutazione d'impatto.
3. I dati personali oggetto di trattamento sono custoditi/memorizzati in locali non accessibili al pubblico (locali tecnici), a cui possono accedere esclusivamente le persone autorizzate al trattamento dei dati, oltre naturalmente l'amministratore di sistema. Non possono accedervi altre persone se non sono accompagnate da soggetti autorizzati.
4. I dati personali oggetto di trattamento sono custoditi/memorizzati come descritto nell'Allegato 2 Dispositivi di salvataggio e memorizzazione (oppure nella documentazione tecnica dell'impianto).
5. La cronologia degli eventi di accesso al sistema di videosorveglianza viene archiviata elettronicamente per almeno sei mesi, mentre l'accesso ai *Server* dotati di *log* di accesso saranno conservati per la durata di almeno sei mesi.
6. In caso di copie di immagini registrate su supporto informatico removibile per le finalità indicate e ai sensi dell'art. 11 "Accertamenti di illeciti ed indagini giudiziarie o di Polizia" il Responsabile interno provvederà a custodirlo in un armadio o simile struttura dotato di serratura fino alla consegna alle autorità competenti, oppure all'eventuale distruzione.
7. Per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto. La cancellazione delle immagini sarà garantita mediante gli strumenti e le procedure tecnologiche più avanzate[2].
8. Nel caso il supporto debba essere sostituito per eccessiva usura, sarà distrutto in modo da renderlo inutilizzabile, in modo che non possano essere recuperati i dati in esso presenti[3].
9. Gli apparati di ripresa digitali connessi a reti informatiche devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale.
10. È garantita la protezione della rete con le misure di sicurezza applicate ai sistemi della Società, anche conformemente a quanto stabilito dal GDPR e dal Garante della protezione dei dati personali.

ARTICOLO 14 - ACCESSO ALLE IMMAGINI

1. Il Responsabile interno e gli incaricati interni ed esterni alla videosorveglianza godono degli stessi livelli di accesso e amministrazione del sistema di videosorveglianza. Ogni utente dispone di accessi personali e risponde ad una specifica profilazione con relativi permessi funzionali.
2. L'accesso alle immagini da parte delle persone autorizzate al trattamento dei dati si limita alle attività oggetto della sorveglianza. Eventuali altre informazioni di cui vengano a conoscenza mentre osservano il comportamento di un soggetto ripreso, non devono essere prese in considerazione.
3. L'accesso alle immagini e ai dati personali è consentito:
   a) al Titolare, al Responsabile interno ed agli Incaricati dello specifico trattamento;
   b) ai preposti alle indagini dell'Autorità Giudiziaria o di Polizia;
   c) all'Amministratore di Sistema dell'Azienda, e alla ditta fornitrice dell'impianto nei limiti strettamente necessari alle loro specifiche funzioni di manutenzione;

[2] Il processo di cancellazione delle immagini presenti sull'NVR è quello descritto sopra. Se ci si riferisce alla conservazione di un'estrazione di tutte o parte di queste, una volta consegnate all'autorità che ne ha fatto richiesta, queste vengono cancellate in modo fisico e non solo logico dai sistemi di memorizzazione utilizzati per il trasporto mediante appositi software. (formattazione del supporto).
[3] I contratti prevedono il comodato d'uso degli apparati. Pertanto, eventuali sostituzioni per danno, manutenzione o aggiornamento, prevedono che il vecchio dispositivo sia prelevato dal proprietario Axitea, previa attesa delle 24 ore per sicurezza dell'avvenuta cancellazione dei dati.

d) all'Interessato, debitamente autorizzato, in quanto oggetto delle riprese. Nel caso di accesso ai dati da parte dell'Interessato questi avrà visione solo delle immagini che lo riguardano direttamente.

4. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati, per iscritto, dal Responsabile interno o dal Titolare.
5. Gli incaricati saranno dotati di proprie credenziali di autenticazione di accesso al sistema (*username* e *password*). Agli incaricati, è affidata la custodia e la corretta conservazione delle proprie credenziali di accesso al sistema di videosorveglianza nell'ambito delle competenze designate.
6. Il sistema dovrà essere fornito di procedure di tracciamento degli accessi (*login* e *logout*), che saranno conservati per un congruo periodo non inferiore a sei (6) mesi.
7. Tutti gli accessi alla visione saranno documentati mediante l'annotazione in un apposito "registro degli accessi" derivante dalla registrazione dei file di log ricavati dal sistema. Qualora il sistema non abbia questa funzione sarà necessario annotare su apposito registro da parte degli incaricati i seguenti dati relativi agli accessi:
   a) la data e l'ora dell'accesso;
   b) l'identificazione del terzo autorizzato;
   c) le eventuali osservazioni dell'incaricato;
   d) l'eventuale export realizzato e le relative motivazioni;
   e) la sottoscrizione del medesimo.

ARTICOLO 15 - CESSAZIONE DELL'ATTIVITÀ DI VIDEOSORVEGLIANZA

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
   a) distrutti;
   b) ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti.
2. La cessione dei dati in violazione al comma precedente è da considerarsi priva di effetti e sono fatte salve le sanzioni previste dalla Legge.

ARTICOLO 16 - DIRITTI DELL'INTERESSATO

1. In relazione al trattamento dei dati personali il Titolare assicura all'interessato l'effettivo esercizio dei seguenti diritti:
   a) 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 personali e alle seguenti informazioni (art. 15 comma 1 del GDPR):
      - le finalità del trattamento;
      - le categorie di dati personali in questione;
      - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
      - quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, criteri utilizzati per determinare tale periodo;
      - l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
      - il diritto di proporre reclamo a un'autorità di controllo

- qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato;

a) il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento dei dati personali ad un paese terzo o a un'organizzazione internazionale ai sensi dell'articolo 15 comma 2 del GDPR;

b) il diritto di ottenere una copia dei dati personali oggetto di trattamento ai sensi dell'articolo 15 comma 3 del GDPR;

c) il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (diritto all'oblio) ai sensi dell'articolo 17 del GDPR;

d) il diritto di ottenere la limitazione del trattamento dei dati personali che lo riguardano ai sensi dell'articolo 18 del GDPR;

e) il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 21 del GDPR;

f) il diritto ad essere informato senza ingiustificato ritardo riguardo alla violazione di dati personali che lo riguardano, quando tale violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche ai sensi dell'articolo 34 del GDPR.

2. Per ciascuna delle richieste di cui al presente articolo 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.
3. I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.
4. Nell'esercizio dei diritti di cui al comma 1 del presente articolo 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.
5. Le istanze di cui al presente articolo possono essere trasmesse al Titolare che dovrà provvedere in merito entro trenta (30) giorni, con proroga a novanta (90) giorni tenuto conto della complessità e del numero delle richieste. Le informazioni in risposta alle istanze dell'interessato sono fornite per iscritto anche attraverso mezzi elettronici e sono gratuite.
6. Al titolare spetta dare riscontro all'interessato e valutare se si tratta di richieste manifestamente infondate o eccessive.
7. Il Responsabile esterno è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati.
8. In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.
9. Nel caso di esito negativo alle istanze di cui al presente articolo, 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.

ARTICOLO 17 - PROCEDURA PER L'ACCESSO ALLE IMMAGINI DA PARTE DEGLI INTERESSATI

1. Per accedere ai dati ed alle immagini l'interessato può presentare istanza scritta all'Azienda all'indirizzo privacy@generalfinance.it richiedendo l'esistenza o meno del trattamento di dati che possano riguardarlo, informazioni sugli estremi identificativi del Titolare e del Responsabile, sulle finalità e modalità del trattamento dei dati, sulla cancellazione, trasformazione in forma anonima o limitazione dei dati trattati in violazione alla normativa vigente in materia, oppure inoltrando la richiesta di opposizione al trattamento dei propri dati personali, per motivi legittimi e documentati, ancorché pertinenti alle finalità del trattamento (articoli 15, 16, 17, 18, 21, 22 e 34 del GDPR).
2. L'istanza deve altresì indicare a quale impianto di videosorveglianza si fa riferimento ed il giorno e l'ora in cui l'istante potrebbe essere stato oggetto di ripresa: nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò dovrà essere data comunicazione al richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione.
3. Il Responsabile interno o un incaricato sarà tenuto ad accertare l'effettiva esistenza delle immagini e darà comunicazione al richiedente. Nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui il suddetto potrà visionare le immagini che lo riguardano.
4. La risposta alla richiesta di accesso a dati conservati deve essere inoltrata entro trenta (30) giorni dalla ricezione (prorogabili a novanta - 90 - giorni) e deve riguardare i dati attinenti alla persona richiedente e può comprenderne eventualmente altri, riferiti a terzi, solo nei limiti previsti dalla normativa vigente.
5. Sono fatti salve tutte le prerogative e i diritti previsti dalla Legge del 7 agosto del 1990, n. 241 e s.m.i. in tema di diritto di accesso agli atti dei procedimenti amministrativi, e previsti dal Decreto Legislativo del 14 marzo del 2013, n. 33 e s.m.i. in tema di diritto di accesso civico semplice e di diritto di accesso civico generalizzato.

ARTICOLO 18 - COMUNICAZIONE DEI DATI

1. La comunicazione dei dati personali acquisiti mediante il sistema di videosorveglianza da parte dell'Azienda favore di altri soggetti autorizzati è ammessa quando necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali.
2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal Responsabile del trattamento e che operano sotto la loro diretta autorità.

ARTICOLO 19 - DIFFUSIONI DEI DATI

1. È in ogni caso fatta salva la comunicazione e la diffusione di dati richiesti in conformità alla legge, da Forze di Polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici per finalità di difesa di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

ARTICOLO 20 - LIMITI ALLA UTILIZZABILITÀ DI DATI PERSONALI

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. (Articolo 22 del GDPR).

CAPO V
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

ARTICOLO 21 - TUTELA AMMINISTRATIVA E GIURISDIZIONALE

La mancata osservanza degli obblighi previsti dal presente Regolamento comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla Legge, di sanzioni amministrative o penali.

ARTICOLO 22 - DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO DI DATI PERSONALI

La materia è regolamentata per l'intero dall'articolo 82 del GDPR e successive modificazioni e/o integrazioni.

CAPO VI
DISPOSIZIONI FINALI

ARTICOLO 23 - MODIFICHE REGOLAMENTARI

I contenuti del presente Regolamento dovranno essere aggiornati nei casi di variazioni delle normative in materia di trattamento dei dati personali, gerarchicamente superiori. Gli eventuali atti normativi, atti amministrativi del Garante per la protezione dei dati personali o atti regolamentari aziendali, dovranno essere immediatamente recepiti.

ARTICOLO 24 - PUBBLICITÀ

Il presente Regolamento entra in vigore dalla data di sottoscrizione da parte del Titolare del trattamento, nella persona del Legale Rappresentante, congiuntamente a quella del Responsabile interno.

ARTICOLO 25 - NORMA DI RINVIO

Per tutto quanto non disciplinato dal presente Regolamento si fa rinvio alle Leggi vigenti, ai provvedimenti attuativi delle medesime, alle decisioni del Garante per la protezione dei dati personali e ad ogni altra normativa, speciale, generale, nazionale e comunitaria in materia di protezione e trattamento dei dati personali nell'ambito della videosorveglianza.

ALLEGATO 1A
ELENCO DELLE TELECAMERE E DELLE ZONE VIDEOSORVEGLIATE

BIELLA CARSO - PIAVE

POSIZIONE	TIPO	DITTA DI ASSISTENZA	MARCA/MODELLO	DESCRIZIONE TELECAMERA	DESCRIZIONE ANGOLO VISUALE	ANNOTAZIONI
Totem Via Carso	Fissa	Axitea	Dahua IPC-HFW5541E-S	2.8 mm fixed lens	Parcheggio privato retro	Parcheggio
Totem Via Carso	Fissa	Axitea	Dahua IPC-HFW4431T-ASE	3.6mm fixed lens	Facciata campo largo	Panorama
Reception	Fissa	Axitea	Dahua IPC-HDW3841TMP-AS	Dome fuoco fisso grandangolare	Porta ingresso dall'interno	Reception
Ingresso Fronte	Fissa	Axitea	Dahua - IPC-HFW5541E-S	2.8 mm fixed lens	Facciata e marciapeide ingress fronte	Ingresso Carso
Ingresso via Piave	Fissa	Axitea	Hikvision	Dome fuoco fisso grandangolare	Scale Ingresso Piave	Ingresso Piave

MILANO

POSIZIONE	TIPO	DITTA DI ASSISTENZA	MARCA/MODELLO	DESCRIZIONE TELECAMERA	DESCRIZIONE ANGOLO VISUALE	ANNOTAZIONI
Ingresso P6	Fissa	Axitea	AXIS - M3106-L	Dome fuoco fisso grandangolare	Ingresso 130°	
Ingresso P7	Fissa	Axitea	AXIS - M3106-L	Dome fuoco fisso grandangolare	Ingresso 130°	
Ingresso P8	Fissa	Axitea	AXIS - M3106-L	Dome fuoco fisso grandangolare	Ingresso 130°	
Cantina P-2	Fissa	Axitea	AXIS - M3025	3.6 mm fixed lens	Ingresso e cantina 91° dall'alto	

ALLEGATO 2
DISPOSITIVI DI SALVATAGGIO E MEMORIZZAZIONE

Indicare da parte dell'Azienda:

- tipologia di dispositivi/i utilizzati per la custodia/memorizzazione delle immagini
  - Milano NVR Hikvision modello DS-7604NI-E1
  - Biella NVR Hikvision modello DS-7708NI-I4

- ubicazione dei dispositivi
  - Milano CED Piano 7
  - Biella CED Piano -1

- misure di sicurezza adottate per ciascun dispositivo
  - Entrambi i device sono collocati in data center con porte sotto controllo accessi. Dal punto di vista del networking operano su una rete segregata dedicata (VLAN e classe di rete) da tutte le altre reti aziendali. La stessa poi per entrambe le installazioni è protetta da un firewall Fortinet per entrambe le sedi. Entrambi i sistemi sono sotto monitoraggio funzionale da parte dell'ufficio Sistemi ICT attraverso soluzione PRTG (Paessler). I dispositivi non risiedono in un eclosure dedicato chiuso a chiave, ma sono collocati nel rack dove ci sono gli altri apparati di rete.