INFORMATIVA PRIVACY VIDEOSORVEGLIANZA

La presente informativa sul trattamento dei dati personali si riferisce al trattamento svolto mediante sistemi di video sorveglianza presso gli stabilimenti e le pertinenze della società Bettinelli F.lli S.p.A., presso le sedi di Bagnolo Cremasco, Via L. da Vinci 56 e Via Milano 33/35

PREMESSA:

L'impianto di videosorveglianza sito nella sede di Via L. da Vinci 56, è dotato di:

a) n. 12 telecamere ad orientamento fisso. Ubicazione telecamere:
01-Parcheggio Visitatori
02- Parcheggio U9-U13-U22
03- Ingresso CB
04- CDS-u5
05- CDS Cancello
06- Parcheggio CB
07- CDS-u4-u3
08- Unità16
09- Lato Nord1
10- Lato Nord2
11- Cancello Ingresso
12- Parcheggio generale

b) n. 1 applicativo su PC per visualizzazione in tempo reale delle immagini degli ingressi "Parcheggio Visitatori" e "Parcheggio CB" ubicato presso il centralino in Unità 15.
n. 1 applicativo per visualizzare e registrare in tempo reale delle immagini di tutte e 12 le videocamere, installato su macchina virtuale all'interno dell'infrastruttura informatica aziendale, situato in unità 15.

c) n. 12 apparecchiatura di registrazione protetta da password.

L'impianto di videosorveglianza sito nella sede di Via Milano 33/35, è dotato di:

a) n. 5 telecamere ad orientamento fisso. Ubicazione telecamere:
01 - Ingresso cancello U21
02 - Ingresso pedonale capannone U21
03 - Parcheggio U21
05 - Retro capannone U21
05 - Ingresso lato nord U21

c) Tutti i dati inerenti alle registrazioni dei registratori saranno salvati e memorizzati per un lasso di tempo di 48 h nella memoria interna degli stessi, l'accesso agli stessi potrà essere effettuato solo dalla Bettinelli F.lli S.p.A. con utenze dedicate protette da un codice di accesso segreto. Infine verrà creata un'utenza alla quale sarà consentito accedere esclusivamente alle riprese live delle telecamere per il controllo dell'area in caso di allarmi o segnalazioni.
Su richiesta della proprietà, al fine di garantire la tutela della privacy, è stata applicata su alcune telecamere la PRIVACY MASK, ciò permette di creare delle zone d'ombra nelle riprese. Una volta che la registrazione viene salvata con questa funzionalità non è possibile rimuovere la zona oscurata, garantendo che la zona vincolata dalla privacy mask non possa essere visionata
Coloro i quali saranno autorizzati a visionare le riprese potranno farlo mediante l'applicazione TRUVISION MOBILE

d) Gli impianti di nostra gestione sono 1 ciascuno dotato di un proprio videoregistratore protetto da codici di accesso

U21 F.LLI BETTINELLI		
componente	quantità	modello
VIDEOREGISTRATORE	1	Aritech TVN-1008s-1T
TELECAMERE	5	Aritech TVB-1101

Le videocamere sono poste, con apposita segnalazione mediante informativa semplificata, nelle zone perimetrali degli stabilimenti e presso gli accessi con logiche di minimizzazione in relazione campo della ripresa, soggetti autorizzati ad accedere alle immagini, durata della registrazione.

La posizione precisa delle telecamere è indicata nelle planimetrie, consultabili a richiesta dell'interessato presso gli uffici del titolare.

Il trattamento dei dati, in conformità a quanto previsto dallo Statuto dei Lavoratori (art. 4, legge n. 300/1970) è stato autorizzato previo Accordo Sindacale con le Organizzazioni Sindacali in data 07/10/20.

1. CHI TRATTA I DATI

Titolare del trattamento è il soggetto che assume le decisioni su come trattare i dati, quindi – tra l'altro – su quali precauzioni prendere per proteggerli, su dove alloggiarli (se in server o cloud, se in modalità cartacea ecc.), su quali dati chiedere al Cliente, su quali elaborare e per quale scopo, su quali e a chi cederli, come gestire i rapporti e i diritti dei Clienti, su chi scegliere come collaboratore, responsabile o semplice incaricato per trattare i dati, su quali istruzioni impartire ai collaboratori ecc... Quindi, dato che il titolare del trattamento dei dati è molto importante, sappia il Cliente che si tratta di:

BETTINELLI F.LLI S.p.A., con sede in Bagnolo Cremasco (CR), Via Leonardo Da Vinci n. 56
P.IVA IT 00984820191
TEL. +39 0373 237411
FAX +39 0373 237538
Email: privacy@bettinelli.it

Poi, per quanto concerne eventuali funzioni accessorie, il Titolare si avvale di soggetti terzi, come incaricati (debitamente autorizzati ed istruiti):

- Dipendenti preposti alla visualizzazione delle immagini;
- Soggetti interni che svolgono funzioni di amministratore del sistema informatico;
- Soggetti interni che svolgono funzioni di manutenzione e riparazione del sistema di video sorveglianza;

2. QUALI DATI VENGONO TRATTATI e QUALI SONO GLI INTERESSATI

I dati che verranno trattati sono i seguenti:

- Immagine della persona;
- Dati ulteriori secondari: dalla visione dell'immagine del lavoratore si possono teoricamente desumere indirettamente informazioni relative alla sua attività lavorativa, come le concrete modalità di esecuzione della prestazione, nei tempi e nei modi, le abitudini ecc. Tali informazioni non sono oggetto di controllo mediante la videosorveglianza.
- Dati ulteriori secondari di terzi: dalla visione dell'immagine di terzi si possono desumere altre informazioni, come la società o ente di appartenenza, l'orario di lavoro, il mezzo eventualmente in uso ecc.

I dati possono riguardare:

- Dipendenti del Titolare;
- Fornitori (o possibili fornitori) del Titolare;
- Collaboratori del Titolare (agenti ecc);
- Clienti (o possibili clienti) del Titolare;
- Terzi che accedono alla sede (Visitatori, corrieri, addetti alle poste ecc).

3. COME VENGONO CONFERITI I DATI E CONSEGUENZE DEL RIFIUTO A CONFERIRLI

Le immagini vengono riprese dagli impianti video.
Il conferimento dei dati è necessario in quanto strettamente strumentale all'accesso ai locali aziendali. In mancanza, il Titolare si troverà nell'impossibilità di far accedere l'interessato ai locali stessi. In ogni caso, ferma la possibilità di visualizzare il cartello di avviso della presenza di un impianto di videosorveglianza, è lasciata all'interessato la facoltà di accedere ed esser ripreso.

4. PER QUALI SCOPI VENGONO TRATTATI I DATI

I dati vengono trattati per le seguenti finalità:

A) **Protezione del patrimonio aziendale**: la funzione dissuasiva delle telecamere e la relativa capacità di documentare eventi funge da deterrente e pertanto ha il fine di proteggere il patrimonio aziendale inteso sia come immobile, sia come beni mobili (compreso il patrimonio immateriale – dati e know how).
Base giuridica: legittimo interesse del datore di lavoro alla protezione e conservazione del patrimonio.

Interessati: terzi, fornitori, collaboratori, clienti e, in caso di atti illeciti, anche dipendenti. Durata della conservazione: 24 ore, salvo proroga in caso di chiusura dello stabilimento (in tal caso le immagini sono conservate per 24 dalla riapertura). In caso di aggressioni (furti, danneggiamenti, accessi non consentiti ecc.) al patrimonio aziendale (anche solo sospette) le immagini sono conservate per un tempo ulteriore e fino ad esaurimento del conseguente contenzioso (ossia fino al termine della conseguente azione civile, penale, amministrativa o disciplinare);

B) **Esigenze organizzative o produttive:** le immagini sono utilizzate per gestire accessi pericolosi o comunque non presidiati o immediatamente visibili per il personale o per gestire flussi di materiali, mezzi o oggetti.

Base giuridica: legittimo interesse del Titolare a garantire la sicurezza delle persone presenti presso la sede aziendale.
Interessati: terzi, fornitori, collaboratori, clienti e dipendenti.
Durata della conservazione: 24 ore, salvo proroga in caso di chiusura dello stabilimento (in tal caso le immagini sono conservate per 24 dalla riapertura). In caso di eventi anomali (furti, danneggiamenti, accessi non consentiti, sinistri ecc.) le immagini sono conservate per un tempo ulteriore e fino ad esaurimento del conseguente contenzioso (ossia fino al termine della conseguente azione civile, penale, amministrativa o disciplinare);

C) **Sicurezza del lavoro:** in caso di accessi a zone pericolose le immagini vengono monitorate per gestire appunto tali accessi.
Base giuridica: salvaguardia interessi vitali delle persone, legittimo interesse del datore di lavoro alla tutela della salute e della sicurezza dei dipendenti e collaboratori.
Durata: 24 ore salvo accessi non autorizzati. In tal caso le immagini sono conservate per un tempo ulteriore e fino ad esaurimento del conseguente contenzioso (ossia fino al termine della conseguente azione civile, penale, amministrativa o disciplinare);

D) **Documentazione sinistri** (assicurazione): nel caso si dovessero verificare sinistri o altri atti illeciti le immagini saranno utilizzate per documentare tali eventi nelle sedi opportune (giudiziarie, di mediazione, extragiudiziarie, assicurative). Base giuridica: legittimo interesse del Titolare. Durata della conservazione: fino ad esaurimento del conseguente contenzioso (ossia fino al termine della conseguente azione civile, penale, amministrativa o disciplinare).

Non è previsto l'utilizzo delle immagini per altre finalità ed in particolar modo è esclusa la finalità di controllo a distanza dell'attività lavorativa.

5. DOVE VENGONO TRATTATI I DATI

I dati personali del Cliente vengono trattati nella sede del Titolare.

6. IN CHE MODO VERRANNO TRATTATI E CONSERVATI I DATI

Tutti i dati personali del Cliente saranno conservati su supporto informatico presso la sede del Titolare compreso l'hosting sul quale appoggia l'applicazione ISPY della sede di via L. da Vinci 56. Per quanto riguarda la sede di via Milano 33/35, i dati personali del Cliente saranno conservati presso la sede del Titolare.
Allego link con informativa privacy valida per tutti gli utenti che si servono delle applicazioni UTC (nel nostro caso Truvision):
https://www.ccs.utc.com/legal/privacy-notice/
Allego link contenente scheda di presentazione per l'applicazione Truvision Mobile:
https://it.firesecurityproducts.com/it/product/video/TVRMobile/82286
I dati sono trattati anche mediante dispositivi mobili con accesso remoto alle immagini.

7. CHI PUÒ ACCEDERE AI DATI E A QUALI SOGGETTI POSSONO ESSERE COMUNICATI

Alle immagini possono avere accesso:

- Dipendenti preposti alla visualizzazione, presso l'azienda o da remoto, delle immagini.
- Soggetti incaricati alla gestione, manutenzione, amministrazione dell'impianto di videosorveglianza;
- Eventuali professionisti che supportano l'azienda con attività consulenziale o legale;
- ASSICURAZIONI;
- Forze di Polizia e/o Autorità giudiziaria, in caso di richiesta.

8. PER QUANTO TEMPO VERRANNO CONSERVATI I DATI

Nella sede di Via L. Da Vinci 43/56, le immagini saranno conservate, per impostazione, per 24 ore.
In caso di chiusura dello stabilimento le immagini sono conservate per 24 ore a decorrere dal momento della riapertura.
Nella sede di Via Milano 33/35, le immagini saranno conservate, per impostazione, per 48 ore.
In caso di chiusura dello stabilimento le immagini sono conservate per 48 ore a decorrere dal momento della riapertura.

In caso di eventi (si veda il punto 4) le immagini saranno ulteriormente conservate fino ad esaurimento del conseguente contenzioso (ossia fino al termine della conseguente azione civile, penale, amministrativa o disciplinare).

9. BASE GIURIDICA DEL TRATTAMENTO

La base giuridica del trattamento è innanzitutto il legittimo interesse del datore di lavoro (vedi punto 4).

10. DIRITTI DELL'INTERESSATO

I clienti sono beneficiari di una serie di diritti.

Innanzitutto il cliente ha diritto di esser informato circa:

- Categorie di dati che vengono trattati (vedi punto n. 2);
- Origine dei dati, ossia sapere da dove il Titolare ha tratto i suoi dati (vedi punto n. 3);
- Finalità del trattamento dei dati, ossia per quali scopi i dati vengono trattati (vedi punto n.4);
- Modalità di trattamento dei dati (vedi punto n. 6);
- Estremi del titolare e di eventuali responsabili del trattamento (vedi punto n. 1);
- Soggetti cui vengono comunicati i dati (vedi punto 7);
- Tempo di conservazione e trattamento dei dati (vedi punto 8);
- Diritto di esperire reclamo innanzi al garante privacy mediante accesso al seguente link: http://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-nostri-dati-personali
- Esistenza o meno di processo di profilazione da parte del Titolare;
- Base giuridica del trattamento (vedi punto n. 9);
- Diritto di revocare il consenso;
- Interessi perseguiti dal titolare mediante il trattamento: esclusivamente quello di svolgere l'incarico affidatogli nel migliore dei modi.

Poi ci sono diritti non di semplice informazione ma operativi:

- **aggiornamento e rettifica**.
- **cancellazione e anonimizzazione**: tale diritto può esser esercitato se i dati sono non più necessari per il fine per cui sono stati trattati.
- **Copia**.

11. PROCEDURA PER ESERCITARE I PROPRI DIRITTI

I diritti elencati al punto precedente potranno essere esercitati dal Cliente inviando una e-mail all'indirizzo privacy@bettinelli.it indicando nel testo quale diritto si vuole esercitare.
Il Titolare deve rispondere entro trenta giorni (che possono esser prorogati di altri due mesi, ma il Titolare in questo caso deve dare avviso motivato del ritardo all'utente).
Il Titolare può rifiutare, se ne ha motivo, di dar seguito alla richiesta dell'utente (rifiuto che deve esser comunicato all'utente entro un mese) solo in caso di richieste manifestamente infondate o ripetitive. Deve dare in tal caso risposta motivata. In ogni caso l'utente può rivolgersi al "Garante Privacy" (si veda link sotto riportato) o al Giudice.
Il Titolare deve rispondere utilizzando lo stesso canale (mail, telefono ecc) utilizzato dall'utente per la richiesta, a meno che l'utente stesso non chieda una risposta per via diversa. In caso di richiesta proveniente da indirizzo email diverso da quello indicato nell'account, il richiedente dovrà provare di esser l'interessato.
Il Titolare, laddove nutra dubbi circa l'identità della persona che avanza la richiesta o esercita uno dei diritti che vengono di seguito elencati, può chiedere ulteriori informazioni per confermare l'identità del richiedente. In caso di richiesta proveniente da indirizzo email diverso da quello indicato nell'account, il richiedente dovrà provare di esser l'interessato.

Le richieste e le risposte sono gratuite, salvo che siano ripetitive. In tale ultimo caso il Titolare può addebitare i costi vivi che affronta per la risposta (quindi costi di personale, costi materiali, ecc).
In ogni caso l'interessato può rivolgersi all'autorità Garante (http://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-nostri-dati-personali) o alla Autorità Giurisdizionale competente per l'esercizio dei propri diritti.

12. IPOTESI DI DATA BREACH
In caso si dovessero verificare, rispetto ai dati, uno o più dei seguenti eventi: accesso, sottrazione, perdita, distruzione, divulgazione, modifica non autorizzati (c.d. Data Breach) il Titolare, ferme restando le misure tecniche urgenti da porre in essere per bloccare (per quanto possibile) l'evento e per ridurne gli effetti dannosi si impegna a:

- ripristinare quanto prima il servizio in modo efficiente, recuperando i dati disponibili dall'ultimo backup utile effettuato;
- informare gli interessati, direttamente se le circostanze lo permettono ovvero genericamente (mediante avviso sull'home del sito web o mediante comunicazione inviata a tutti gli utenti, compresi quelli per i quali eventualmente non ci sono stati eventi sui dati) del tipo di evento, del tempo in cui si è verificato, delle misure adottate (senza entrare nel dettaglio al fine di non agevolare eventuali nuovi attacchi) per ridurre i danni e per evitar nuovi analoghi eventi, nonché delle misure ed accorgimenti che l'utente dovrebbe – da parte sua - porre in essere per ridurre le probabilità di nuovi eventi e limitare le conseguenze di quelli già verificatisi.

Testo in vigore da ottobre 2020

Video surveillance privacy policy

This information regarding the processing of personal data refers to the processing carried out by means of video surveillance systems at the plants and appliances of Bettinelli F.lli S.p.A., at its offices in Bagnolo Cremasco, Via L. da Vinci 56 and Via Milano 33/35

FOREWORD:

The video surveillance system located in the headquarters in Via L. da Vinci 56, is equipped with:

a) n. 12 cameras with fixed orientation. Position of cameras:
   01-Visitor Parking Area
   02- U9-U13-U22 Parking Area
   03- CB Entrance
   04-CDS-U5
   05- CDS Gate
   06- CB Parking Area
   07-CDS-U4-U3
   08-UNIT16
   09- NORTH SIDE 1
   10- NORTH SIDE 2
   11- Entrance Gate
   12- General parking area

b) 1 PC application for real-time viewing of the images of the "Visitor Parking" and "CB Parking" inputs located at the switchboard in Unit 15.
   1 app for real-time viewing of the images of all 12 cameras, installed on virtual machines inside the company informatics infrastructure, located in unit 15.

c) 12 password-protected recording devices.

The video surveillance system located in Via Milano 33/35 is equipped with:

a) 5 cameras with fixed orientation. Position of cameras:
   01 - U21 Entrance gate
   02 - U21 Pedestrian entrance to warehouse
   03 - U21 Parking Area
   04- U21 Rear of warehouse
   05- U21 North entrance

b) All data regarding recordings will be saved and stored in the internal memory of the recorders for a maximum of 48 hours. Access to this data may be carried out only and exclusively by Bettinelli F.lli S.p.A. by means of a secret password. Last but not least, an access point will be created to allow only to access live video footage from the cameras to control areas in the event of alarms or reports. PRIVACY MASKS have been applied to some cameras, creating concealed areas in the videos, in order to ensure the protection of privacy, requested by the owner. Recordings saved with this feature cannot have the concealed area remove, ensuring that the area protected by the Privacy Mask cannot be viewed. Those authorised to view the footage will be able to do so using the TRUVISION MOBILE application

c) The facilities under our management are each equipped with its own video recorder protected by access codes

U21 F.LLI BETTINELLI		
component	quantity	model
VIDEO RECORDER	1	Aritech TVN-1008s-1T
VIDEO CAMERAS	5	Aritech TVB-1101

The cameras, equipped with special signalling by means of simplified information, are positioned along the perimeter areas of the plants and at access points with minimisation logic in relation to the filming area, subjects authorised to access the images, duration of registration.
The precise position of the cameras is indicated in the floor plans, which can be consulted on request of the data subject at the offices of the Data Controller.

The processing of data, in accordance with the provisions of the Workers' Statute (art. 4, law no. 300/1970) has been authorised by prior trade union agreement with the trade unions on October 7th, 2020.

1. DATA CONTROLLER

The **data controller** is the person who makes the decisions regarding how to process the data, therefore - among other things - on which precautions to take to protect said data, where to store it (on a server or cloud, in paper format, etc.), which data to request from the Customer, which data to process and for what purpose, which and to whom to transfer the data, how to manage the relationships and rights of Customers, who to choose as a collaborator, manager or simple person in charge of processing the data, which instructions to give to collaborators etc. ... Therefore, given that the data controller is extremely important, the Customer must be informed that said controller is:
BETTINELLI F.LLI S.p.A., with headquarters in Bagnolo Cremasco (CR), Via Leonardo Da Vinci n. 56
Italian VAT number IT 00984820191
TEL. +39 0373 237411
FAX +39 0373 237538
Email: privacy@bettinelli.it

The Owner also makes use of assigned, instructed and authorised third parties, with regard to ancillary functions, as follows:
- Employees in charge of viewing the images;
- Company personnel who carry out IT system administrator functions;
- Company personnel who carry out maintenance and repairs on the video surveillance system;

2. WHICH DATA IS PROCESSED and WHO ARE THE INTERESTED PARTIES

The following data is processed:
- Images of people;
- Secondary data: from the vision of the worker's image it is theoretically possible to indirectly infer information relating to his work, such as methods of execution, timing and manner, habits, etc. This information is not subject to control by means of video surveillance.
- Additional secondary data regarding third parties: other information, such as the company or organisation to which they belong, working hours, the means in use, etc., can be deduced from the images of third parties.

Said data may concern:
- Employees of the Data Controller;
- Suppliers (or possible suppliers) of the Data Controller;
- Collaborators of the Data Controller (agents, etc.);
- Clients (or possible clients) of the Data Controller;

- Third parties who have access to the premises (Visitors, shippers, post office workers, etc.).

3. HOW THE DATA IS COLLECTED AND CONSEQUENCES OF THE REFUSAL TO PROVIDE IT

The images are taken by the video systems.
Data collection is necessary as it is fundamental in order to access company premises. The Data Controller will not be able to allow the interested party to access the company if said data is not provided. In any case, since the interested party has the possibility of viewing the informative sign indicating the presence of a video surveillance system, he also has the responsibility of deciding whether to access the premises and be filmed or not.

4. WHY DATA IS PROCESSED

Data is processed for the following reasons:

a) **Protection of corporate assets**: the preventive function of cameras and the possibility of recording events acts as a deterrent and, therefore, protects corporate assets intended both as fixed property and as movable assets (including intangible assets - data and know-how).
Legal basis: legitimate interest of the employer in the protection and conservation of assets.
Interested parties: third parties, suppliers, collaborators, customers and, in the case of illegal acts, also employees.
Duration of storage: 24 hours, unless extended in the case of closure of the establishment (in this case the images are stored for 24 hours after reopening). In the event of aggression (theft, damage, unauthorised access, etc.) to company assets (even if only suspicious), the images are stored for a longer time and, in any case, until the consequent litigation is terminated (i.e. until the end of the consequent civil-, criminal-, administrative or disciplinary litigation);

b) **Organisational or productive needs**: images are used to manage dangerous or unattended access or immediately visible to staff or to manage flows of materials, vehicles or objects.
Legal basis: legitimate interest of the Data Controller in order to guarantee the safety of the persons present in the company's premises.
Interested parties: third parties, suppliers, collaborators, customers and employees.
Duration of storage: 24 hours, unless extended in the case of closure of the premises (in this case the images are stored for 24 hours after reopening). The images are stored for an additional period and until the consequent litigation is concluded (i.e. until the end of the consequent civil, criminal, administrative or disciplinary action) in the case of anomalous events (theft, damage, unauthorised access, accidents, etc.);

c) **Safety in the workplace**: images are monitored to manage accesses to dangerous areas.
Legal basis: safeguarding the vital interests of individuals, legitimate interest of the employer in protecting the health and safety of employees and collaborators.
Duration: 24 hours except for unauthorised access. In this case, the images are stored for an additional period, and until the consequent litigation is concluded (i.e. until the end of the consequent civil-, criminal-, administrative- or disciplinary action);

d) **Claims documentation** (insurance): the images will be used to document accidents or other unlawful acts in the appropriate offices (judicial, mediation, extra-judicial, insurance). Legal basis: Duration of storage: until the consequent dispute is concluded (i.e. until the end of the consequent civil-, criminal-, administrative- or disciplinary action).
The use of the images for other purposes is not foreseen, and the remote control of work activities, in particular, is excluded.

5. WHERE DATA IS PROCESSED

The personal data of Customers is processed at the offices of the Data Controller.

6. HOW DATA IS PROCESSED AND STORED

The personal data of Customers is stored on IT support at the headquarters of the Data Controller, including the hosting that supports the ISPY application of the offices in via L. da Vinci 56. The personal data of Customers is stored at the offices of the Data Controller with regards to the offices in via Milano 33/35.

The following link provides privacy information valid for all users who use UTC applications (in our case Truvision):
https://www.ccs.utc.com/legal/privacy-notice/
The following link provides the presentation sheet for the Truvision Mobile application:
https://it.firesecurityproducts.com/it/product/video/TVRMobile/82286
Data is also processed by means of mobile devices with remote access to images.

7. WHO CAN ACCESS THE DATA AND WHO SAID DATA CAN BE COMMUNICATED TO

Images can be accessed by:

- Employees in charge of viewing the images at the company or remotely.
- Subjects in charge of the management, maintenance, administration of the video surveillance system;
- Professionals who provide the company with consultancy or legal activities;
- INSURANCE:
- Police force and/or judicial authorities, if requested.

8. DURATION OF DATA STORAGE

Images are stored, by default, for 24 hours at the offices in Via L. Da Vinci 43/56.
In the case of closure of the premises, the images are stored for 24 hours after reopening.
Images are stored, by default, for 48 hours at the offices in Via Milano 33/35.
In the case of closure of the premises, the images are stored for 48 hours after reopening.
In the case of events (see point 4), the images will be stored for an additional period until the consequent dispute is concluded (i.e. until the end of the consequent civil-, criminal-, administrative- or disciplinary action).

9. LEGAL BASIS OF THE PROCESSING

The legal basis of the processing is, above all, the legitimate interest of the employer (see point 4).

10. DATA SUBJECT RIGHTS

Customers benefit from a series of rights.
First and foremost, customers have the right to be informed about:

- Categories of data processed (see point n. 2);
- Origin of the data, i.e. where the Data Controller obtained his data (see point n. 3);
- Purpose of data processing, i.e. for which purposes the data is processed (see point n. 4);
- Methods of processing data (see point n. 6);
- Details of the data controller and any data processors (see point n. 1);
- Persons to whom the data is communicated (see point 7);
- Data storage and processing time (see point 8);
- The right to lodge a complaint with the Data Protection Supervisor by accessing the following link: http://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-nostri-dati-personali
- Existence or otherwise of profiling process carried out by the Data Controller;
- Legal basis of the processing (see point n. 9);
- Right to withdraw consent;
- Interests pursued by the data controller through processing: exclusively to carry out the task

- entrusted to him in the best possible way.

There are also rights that are not just information but operational:

- **updating and correction**.
- **cancellation and anonymisation**: this right can be exercised if the data is no longer necessary for the purpose for which it was processed.
- **Copy**.

11. HOW TO EXERCISE YOUR RIGHTS

The rights listed in the previous point may be exercised by Customers by sending an email to privacy@bettinelli.it indicating which right they want to exercise.
The Data Controller must reply within thirty days (which may be extended by another two months, but, in this case, the Data Controller must give a reasoned notice of the delay to the user).
The Data Controller may refuse, if he has reason, to comply with the user's request (refusal that must be communicated to the user within a month) only in the case of requests that are manifestly unfounded or repetitive. In this case he must give a reasoned reply. In any case, the user may contact the "Privacy Guarantor" (see link below) or the Judge.
The Data Controller must respond using the same channel (mail, phone, etc.) as that of the user in his request, unless the user himself requests a different response. In the event of a request from an email address other than that indicated in the account, the applicant must give proof that he is the interested party.
If and when the Data Controller has doubts about the identity of the person making the request or exercising one of the rights listed below, he may request further information to confirm the identity of the applicant. In the event of a request from an email address other than that indicated in the account, the applicant must give proof that he is the interested party.

Requests and replies are free of charge, unless they are repetitive. In the latter case, the Data Controller may charge the extra costs he faces for the response (i.e. personnel costs, material costs, etc.).
In any case, the interested party may contact the Privacy Guarantor (http://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-nostri-dati-personali) or Judge responsible for the exercise of their rights.

12. HYPOTHESIS OF DATA BREACH

Should one or more of the following events occur with respect to the data: unauthorised access, theft, loss, destruction, disclosure, modification (so-called Data Breach), the Data Controller, without prejudice to the urgent technical measures to be put in place to block (as far as possible) the event and to reduce its harmful effects, undertakes to:

- reactivate the service efficiently as soon as possible by recovering the available data from the last useful backup carried out;
- inform the interested parties, directly if circumstances permit or generically (by means of a notice on the homepage of the website or by means of a communication sent to all users, including those for whom there may have been no events regarding their data) concerning the type of event, the time in which it occurred, the measures taken (without going into detail, so as to limit the possibility of new attacks) to reduce the damage and to avoid new similar events, as well as the measures and precautions that the user should – for his part – put in place to reduce the probability of new events and limit the consequences of those that have already occurred.