FRANZOSINI / FIDI DATA (PRIVACY) PROTECTION MANAGEMENT

(FAIM) v. 3.2
DECEMBER 2020

Contents

Owners of data / interested individual. 3

Methods of obtaining data. 3

Purposes for obtaining, using, retaining or disclosing of data. 4

Methods of retaining/recording data and location. 4

Review and update of personal information 5

Retention period and destruction 5

Providing data (Notice, choice and consent) 5

Protection of data. 6

Transmittal of data. 6

Electronic Distribution of data. 7

Distribution to **third parties.** 7

Monitoring and review process 7

Complaints and disputes 7

Available systems (where possible) 8

Data storage security procedures and processes 8

Distribution (any official copies over and beyond the original) 8

All personal information covered by the law and recorded either in writing or on electromagnetic media (hard disks (server or PCs), CDs, tapes, back up media etc.) is subject to this procedure which per indications which personal data is managed, where it comes from and with whom it has been shared.

Here you are the overview of all data processing activities.

Data shall be requested for each individual business transaction regardless of whether the data is already in our possession.

Owners of data / interested individual.

Owners of data are:

1. direct Franzosini employee and management personnel; and

2. customer / client (the information such as passport details, tax id, address, phone number, email)

3. agents and third parties operating on Franzosini's behalf

Methods of obtaining data.

Data is obtained orally and in writing.

Data is collected orally during the course of conducting business telephonically or in person (office visits) (e.g. requests for information, requests for quotation etc.).

Written data is collected during conduct of business through normal correspondence or using electronic means (e-mail, transfer applications – drop box, we transfer, CD's, tapes, etc.)

Purposes for obtaining, using, retaining or disclosing of data.

1. Employees.

Data on employees is necessary to comply with the formalities required by law, regulations and Community legislation concerning the administration of employees, such data will be processed on paper and/or magnetic, electronic, and similar media, and in any case using instruments that guarantee security and confidentiality.

2. Customer/client.

Client's data is required and used exclusively for the following purposes:

- the establishment or continuation of a business contractual relationship;
- to comply with proper administrative procedures, civil, fiscal and other requirements of law;
- commercial and marketing statistics;
- to answer questions;
- to maintain and update a most frequently asked questions, proposals and communications database
- for eventual subscription to our newsletter whenever available;

Methods of retaining/recording data and location.

It's important to maintain accurate, complete and relevant personal information.

Franzosini Srl records data both in written (physical) and electronic form.

Written data is found in personnel files, customer service files, accounting files, reports and other documentation required by law, regulation, community legislation or governmental entities.

Data obtained orally is normally reduced to written form subsequently placed in the above mentioned files.

Electronic form of data is retained on the server or on individual PCs.

Electromagnetic recording of oral data is not required nor permitted at Franzosini Srl.

Review and update of personal information

Review and update of personal information is not allowed nor from private customer nor from corporate account since it used for single move only and shall be requested foreach individual business transaction regardless of whether the data is already in our possession.

Retention period and destruction

Employee and management personal data is maintained for the duration of employment or appointment and destroyed upon termination of employment or cessation of the appointment.

Customer/client personal data is maintained for the period as indicated in article 2220 of the civil code (10 years) and then destroyed.

All documents are destroyed in a manner to render impossible any subsequent restoration of the personal data or sensitive date. This is accomplished using means such as paper shredders or incinerators but in no way trash cans unless the documents are reduced to a form that impedes the reconstruction of the information that they initially contained.

Data stored on electromagnetic media shall be destroyed through permanent cancellation from the storage media. Back up data will likewise be deprived of availability of all personal data previously destroyed/cancelled.

Providing data (Notice, choice and consent)

The interested party/owner of the data shall be provided an express choice concerning the consent or otherwise to the collection and use of data, to include disclosure.

This is done by re-directeng the client to our website where he / she can consult both our Privacy Protection Policy and our ABC charter. These enclosures include a consent choice for completion by the data owner. The enclosures also inform the owner of the consequences, if consent is not given directly, in the absence of particular comments or requests regarding data protection Franzosini will operate on an implicit consent basis, taking for granted that the customer has read the information regarding data protection provided in the documents.

Whenever possible and practicable in conducting business orally, Franzosini staff informs the client of the consent choice and that if consent is not given or in case of failures in providing the specifically requested data, even partially, places Franzosini Srl in the impossibility to fulfil their requests as we cannot complete required processes and laws.

Protection of data.

a. All physical forms of data shall be kept in appropriate types of filing media to the maximum extent possible and kept solely in designated areas that are constantly surveilled during normal operating hours. After duty hours these areas are subject to both electronic anti intrusion surveillance and detection supported by random intrusion detection patrols.

Areas where personal data is maintained will so be indicated with appropriate cautionary signs.

Custody of this data is the responsibility of personnel assigned to perform the related duties and those located in the vicinity of the storage location. Personnel other than those charged with administrative or management duties will be challenged as to their need to know personal data before they can access files or systems where personal data is kept.

Sensitive data will be kept under key and in the custody of the person responsible for the function. Access or disclosure of these sensitive data will only be permitted to management personnel and personnel with a verified need to know and necessary to perform specifically assigned duties/responsibilities.

b. Data stored on electronic media is protected from unauthorized access and disclosure through use of credential authenticating application (password) which permit passing an access screening procedure.

Sensitive data is further protected by being kept in directory folders that have a second authenticating control which permits access only to designated personnel maintained by the systems manager. Sensitive data will not be kept in electronic form in generic directory folders that do not have the secondary authenticating control.

c. Access to the warehouse where forwarding/storage data is evident requires authorized entry. Unescorted entry is authorized for Franzosini Srl employees and certain suppliers strictly for performance of assigned duties and services respectively. The warehouseman will maintain a list of authorized personnel for unescorted entry. All other personnel require escorted entry by the warehouse man or other authorized employee***.***

In case of violation of above procedure it's Franzosini's responsibility to inform the Postal Police (for digital unauthorized access) or Police / Carabinieri (for physical unauthorized access) for further investigation and actions taking as per applicable laws and regulations

Transmittal of data.

All e-mails and other correspondence with or transmitting data will include an appropriate statement concerning the confidentiality, restricted use to the intended addressee and notification concerning misdirection of the correspondence and warning against any type of further unintended processing of the contents.

Electronic Distribution of data.

The PEC e-mail is the preferred system whenever transmitting personal sensitive or judicial data using electronic means. The PEC system is the equivalent of certified mail return receipt.

Distribution to third parties.

Some personal data may have to be distributed to those third parties involved in the process of the move such as local origin agents, customs agents or destination agents. Most commonly this happens through the sending of the documents required by each party to perform their service (eg. Copy of the passport and of the Italian fiscal code will be sent to the customs agent so as to allow preparation the documents for an FCL shipment).

In no case will any data other than that specifically required be distributed to any person or party involved.

Franzosini forbids and prevents its members from distributing or seeking any data other than that they duly came into possession.

Should personal data be requested through official channels by the police forces or other law enforcement agencies, Franzosini will second the request in compliance with the law in force.

Monitoring and review process

Monitoring and enforcement of the Privacy policy and procedure of Franzosini is the responsibility of all personnel, but in particular the administrative personnel that as part of their duties obtain, use and maintain files with personal data.

Agents and third parties operating on Franzosini's behalf have been chosen also taking into account their respect for Privacy. Therefore when data is disclosed, such parties are required and expected to operate following the specifications of our policies or similar policies, edited on the basis of Italian laws and of the laws in force in the subject country for services abroad.

During internal audits/inspections the applicability of this procedure shall be verified and reported to management. The verification process shall include examination of files for correspondence to the requirement herein established as well as electronic systems access/security.

The Privacy policy and procedure of this document shall be reviewed at least annually and updated as necessary. It shall also be reiterated to dependent personnel once a year.

Complaints and disputes

All complaints involving personal data will be directed/addressed to and handled by the Managing Director of Franzosini Srl.

Any resulting disputes will be processed in accordance with Italian law decree 196/03 depending on the type of data involved in the dispute.

Available systems (where possible)

PCs and Servers

Data storage security procedures and processes

Procedure

The administration for Franzosini business is done by a computer network based on one Server station and different workstations.

The hardware can be of different suppliers. The software is based on Microsoft Windows applications for which licenses are available.

Some independent programs are also available for which no license is required.

Processes

a) Back-ups

   Copy of all data is stored on two external hard disks. The primary and secondary back up of the server are done remotely by Syplus.

b) Security control

   - Some programs are secured as read only, they can only be changed by server operations.
   - All programs are authorized for all the users except for bookkeeping programs, salary registrations etc. which are only accessible by the administration person.
   - Antivirus program (Norton) is used and one firewall (Gigasys) – entry and exit through server.

Distribution (any official copies over and beyond the original)

None