

Information required by Regulation (EU) 2016/679

PREMISE

Friulpress-Samp SpA considers the protection of personal data of fundamental importance, ensuring that processing takes place in full compliance with the protections and rights recognized by Regulation (EU) 2016/679 (hereinafter the "*Regulation*" or "*GDPR*"), by other national and EU rules as well as the provisions of the data Protection Authorities. The processing of personal data operated by **Friulpress-Samp SpA** is inspired by the principles of lawfulness, correctness and transparency and Data Controller uses the minimum set of data for the strictly necessary period of time. **Friulpress-Samp SpA** processes data as accurate and up to date as possible, preserving security and as established in GDPR, following principle of transparency, and provides the following information.

| | | |
|--|--|--|
| | Data Controller Friulpress-Samp SpA | Friulpress-Samp SpA Zona industriale 5 33079 Sesto al Reghena (PN) Tel: +39 0434-693211 |
| | Data Protection Officer (DPO) | Data Protection Officer c/o Friulpress-Samp SpA DPO@HDT-IT2.com |

ORIGIN AND TYPE OF PERSONAL DATA PROCESSED

The data is collected directly from the Data Subject or by the company/entity to which a service contract is in place. Where required by law, with protection of professional secrecy, it is possible that data relating to the possession of particular qualifications or the absence of criminal proceedings and convictions (art. 10 of the GDPR) as well as personal data governed by art. 9 of the GDPR (so called "*special categories of personal data*")¹ as in the case where biometric data are required for access to protected areas and systems. The processing, however, complies with the principle of data minimization and storage limitation.


The personal data processed include the following:

- personal and tax details;
- contact details (mobile, landline, email);
- bank or postal account details;
- data relating to the study curriculum and professional path;
- data relating to health conditions (illness, injury, allergies, ...);
- data relating to trade union or political membership (if the activation of particular forms of protection is requested such as, for example, to become leaved or posted employee,...);
- data relating to: the tasks (time and quantity of output) and the role played in the organisation; remuneration; behavior in the workplace that is subject to disciplinary action; data relating to the entrusted work tools, including vehicles in use;
- images and voice.

Unless otherwise specified, the data will be processed for 10 years and, subsequently, for the maximum time established by the applicable legal provisions regarding the limitation of rights and/or expiration of the action and, in general, for the exercise/defense of the rights of the Data Controller in disputes brought by or against public authorities, public entities/bodies and private entities.


The data will be processed, however, for the entire duration of the trial in every phase and degree.


¹Article 9 of the GDPR considers data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".


| When processing is permitted for the legitimate interests of Data Controller , it refers solely to: the protection of company assets and resources; to verify the correct functioning of the assigned resources and to prevent or verify damage to company systems; the need to trace precise responsibilities for violations of the law, regulations or procedures; to prevent or prosecute inappropriate and/or fraudulent behavior. | | | |
|---|--|---|--|
|  | PURPOSE | LEGAL BASIS | NOTES & RETENTION TIMES |
| | <i>Establishment and Administrative Management of the Work/Collaboration Relationship, payment of contributions and tax withholdings</i> | <i>Legal obligation (art. 6.1.c) and 9.2.b) - (art. 43 Presidential Decree 600/73 and art. 2220 CC)</i> | <i>The administrative management of the Employment Relationship requires the conservation of accounting records in order to certify the fulfillment of tax, salary and social security obligations. Data relating to health may also be processed for the definition of suitability judgments, the management of accidents and illnesses, maternity/paternity leave, the onset of particular pathologies or membership of protected categories as well as other data forming part of a set that the GDPR, in art. 9, defines "particular categories of personal data". Budget data are kept for up to 10 years from the last payment, as required by law. The data relating to the conditions that determined the hiring and/or relating to pathologies or consequences of accidents are processed for the maximum time established by the applicable legal provisions regarding limitation of rights and/or expiry of the action and, in general, for the exercise/defense of the Owner's rights.</i> |
| | <i>Management of employee skills and training</i> | <i>Legal obligation (art. 6.1.c) - Legislative Decree 81/08, as amended and Legislative Decree. 152/06 or other for compulsory training Consent (art. 6.1.a) for non-compulsory training</i> | <i>The employer must assign only trained personnel to certain specific tasks as a result of certain legislative provisions and binding obligations. In other cases, training is optional but allows employees to develop their full potential. The data is stored for the entire duration of the collaboration relationship.</i> |
| | <i>Payment of salaries and skills</i> | <i>Employment Contract (art. 6.1.b) - and Legal Obligation (art. 6.1.c, 9.2.b) - (art. 2220 CC)</i> | <i>Payment of emoluments takes place via bank transfer or other tracked instruments and the Data Controller may become aware of the bank details, as governed by the contract stipulated with the collaborator. The data is stored for 10 years from the last payment, as required by law.</i> |
| | <i>Benefits</i> | <i>Employment contract and collective company agreements (art. 6.1.b);</i> | <i>The Data Controller is required to process data in accordance with collective and company agreements. The data is kept for 10 years from the termination of the employment relationship</i> |
| | <i>Communication of data to control bodies in case of contributions</i> | <i>Legal obligation (art. 6.1.c)</i> | <i>In the case of disbursement of contributions, the legislative and regulatory provisions require the sending of reports of the expenses incurred to national, regional or local control bodies. The data is stored for up to 10 years after provision, for administrative purposes only.</i> |
| | <i>Work Organization</i> | <i>Employment Contract (art. 6.1.b)</i> | <i>Presence, roles and tasks are processed for the purposes of exercising the employer's powers of work organization.</i> |

| | | |
|---|---|--|
| | | <p>Their communication to external parties is aimed at managing work activities and operational flow, or managing institutional and commercial relationships. The data may be disclosed in the organizational charts both on the pages of the Data Controller's website and in the organizational charts or in communications to collaborators and business partners.</p> <p>Any photos to identify the figures represent a tool for improving communication and, in general, the relationship with company interlocutors and business partners.</p> <p>The data is stored for at most the entire duration of the employment/collaboration relationship.</p> |
| Hygiene and Safety at Work | <p>Legal obligation (articles 6. 1.b , 9.2.b and 9.2.h) – Legislative Decree 81/08, as amended ; DM 155/08; Legislative Decree 230/95.</p> | <p>The legislation on the protection of health and safety at work requires the retention of data relating to employees and collaborators. The data is mainly contained in health and risk records which have a minimum mandatory content (Annex 3A of Legislative Decree 81/08) as well as in appropriate mandatory registers (complaints, single labor register, ...).</p> <p>The data is kept for at least 10 years from the termination of the employment/collaboration relationship (Art. 25, paragraph 1, letter e of Legislative Decree 81/08).</p> <p>In the case of subjects exposed to carcinogenic or mutagenic agents or asbestos dust, health data are stored in the company for the entire duration of the employment relationship and at INAIL for a period of 40 years from the termination of the employment relationship (art. 3 Ministerial Decree 155/07).</p> <p>In the case of subjects exposed to ionizing radiation, the exposure data must be kept for at least five years from the end of the employment relationship (Legislative Decree 230/95) and transmitted to INAIL which keeps them for 30 years.</p> |
| Management of Log Files only for those who hold the role of System Administrators | <p>Legal obligation (art. 6.1.c) – Provision. 27/11/08 of the Guarantor on System Administrators</p> | <p>The term "system administrator" refers to both professional figures who deal with the management and maintenance of a data processing system or its components, as well as database administrators, network administrators and security that administrators of complex software systems.</p> <p>For them, the recording of time references and the description of the event that generated the accesses is foreseen.</p> <p>The records must be kept for a period of no less than six months and are subjected to an audit on an annual basis.</p> <p>The list of individuals designated as system administrators for personnel data can be made known to all collaborators who request it.</p> <p>The data is kept for one year and, if behaviors and/or omissions worthy of attention emerge, the data is kept for the legally significant period.</p> |
| Compliance with instructions on the use of company tools and assets | <p>Legitimate interest of the Data Controller (art. 6.1.f).</p> | <p>The methods of correct use of company tools and the related analyzes on compliance with what has been established are carefully described in the</p> |

| | | |
|--|--|---|
| | | <p>appointment as person in charge (processing authorization)</p> <p>The data is kept for 6 months from the termination of the employment relationship.</p> |
| <p>Mobile phones, smartphones and tablets and laptops and other company devices</p> | <p>Legitimate interest of the Data Controller (art. 6.1.f).</p> | <p>No continuous data on the user's location is collected in covert mode. The use of apps is not monitored and no programs are installed for performance monitoring purposes nor are the contents of communications monitored.</p> <p>The only control foreseen concerns any malware or to guarantee the security of the Owner's network and information system.</p> <p>In the case of mobile phones, part of the number contacted and some data relating to the call appear attached to the invoice.</p> <p>The data is stored only as attachments to the accounting documentation for the requested topics (10 years).</p> |
| <p>Exercise of a right in court for the defense of the interests of the Data Controller and its Customers and/or the analysis of legally significant events</p> | <p>to ascertain, exercise or defend a right in court (art. 9.2.f).</p> | <p>This practice may also involve analysis of backup copies of the data.</p> <p>The data is kept for the maximum time established by the applicable legal provisions regarding the limitation of rights and/or expiration of the action and, in any case, for the entire duration of the judgment in all its phases and degrees.</p> |
| <p>Voice and images for activity documentation, institutional communication, employer branding and business development. CV data</p> | <p>Legitimate interest of the Data Controller (art. 6.1.f) for the publications consent (art. 6.1.a) for other cases</p> | <p>Any television filming in the workplace to document activities or operations solely for dissemination or institutional or corporate communication purposes, and which involve employees and collaborators, can be assimilated to temporary treatments aimed at the occasional publication of articles, essays and other events of thought. In this case, the provisions on journalistic activity contained in Legislative Decree 196/03 (articles 136 et seq.) apply to them, without prejudice, however, to the limits to the right to freedom of the press placed to protect confidentiality, as well as observance of the code of ethics for journalistic activity and the right of the worker to protect his own image by opposing, for legitimate reasons, its dissemination (Guarantor - Provision regarding video surveillance - 04/08/10). By analogy, the photos and the voice are also subject to the same regime in the case of publications.</p> <p>The dissemination on the site, on social networks, on business cards or on the noticeboard, of photos or data relating to the professional curriculum represents a tool for improving communication and, in general, the relationship with corporate and institutional interlocutors and business partners as well as with possible contacts. For this, however, specific consent is required.</p> |
| <p>Management of data relating to family members and cohabitants for the granting of legal concessions and benefits, the response to administrative obligations and the payment of payments.</p> | <p>Legal obligation (art. 6.1.c) for employees and collaborators Consent (art. 6.1.a) for family members and cohabitants</p> | <p>In granting benefits granted by law to employees and collaborators, as well as in responding to administrative and tax obligations, the Data Controller processes not only the data relating to this category of interested parties but also of family members and cohabitants.</p> <p>In relation to the latter, specific consent is required.</p> |

| | |
|---|------------------------------------|
|  | MANDATORY PROVISION OF DATA |
| <p>Most of the data is collected by virtue of contractual clauses or legal obligations and, only in some cases, consent is required. Its absence, depending on the case, will lead to consequences linked to the purpose for which data was collected such as, for example, the impossibility of participating in training courses that are not mandatory by law.</p> | |

| | |
|--|--|
|  | RECIPIENTS AND SUBJECTS AUTHORIZED TO PROCESS |
| <p>The personal and contact data as well as its role in the organization may be communicated and known by subjects who have established or intend to establish a commercial relationship or who have institutional relationships with the Data Controller, solely to contribute to the achievement of the Data Controller institutional purposes. Without prejudice to the communications and disseminations carried out in execution of contractual obligations, those ordered by orders of the Authorities or required by law, assuming that communication to third parties does not exempt the latter from providing the information and from asking for consent to the processing, it is specified that the data may be communicated to:</p> <ul style="list-style-type: none"> • Banks, post offices and companies issuing credit/debit cards; • Insurance and insurance brokerage companies, appraisers; • Control bodies, including internal ones, and auditors; • Public Bodies and Authorities (INPS, INAIL, National Labor Institute, District Employment Sections, Tax Offices, Public Security Authorities, ASL; ARPA; Regional Offices; ...); • Companies, individual entrepreneurs and professionals with whom Data Controller has supply relationships of goods and services, commissioning, contracting, subcontracting or that intervene in the same workplace; • Companies offering transport, hotel accommodation and catering services; • Trade union organisations, CAAF, funds or even private social security and assistance funds which have been given an explicit mandate; • Relatives and acquaintances (<i>however, a written delegation is required</i>); <p>The data may be processed by subjects qualified as Data Processors pursuant to art. 4.8 and art. 28 of the GDPR (professionals, lawyers, consultancy and service companies, hardware and software assistance companies, Parent Company or controlled and associated companies, ...) and by subjects authorized to process pursuant to art. 29, who operate under the direct authority of the Data Controller who has instructed them in this regard (employees and collaborators).</p> <p>The list of subjects qualified as "System Administrators" for data relating to personnel management is available from the Data Controller.</p> | |

| | |
|---|---|
|  | TRANSFER OF PERSONAL DATA TO COUNTRIES NOT BELONGING TO THE EUROPEAN UNION |
| <p>The Data Controller makes use of professional services offered by some suppliers, adequately qualified as Data Processors. This may result in the data being transferred outside the EU territory but only:</p> <ul style="list-style-type: none"> • towards countries subject to an adequacy decision by the European Commission or the Guarantor (art. 45 of the GDPR); • in countries located outside the EEA, subject to signing the Standard Contractual Clauses adopted/approved by the European Commission pursuant to art. 46, 2, letter. c) and d). In the event that this occurs, a copy of the guarantees referred to in art. 46, par. 2, letter. c) and d), used by the Data Controller can be obtained by writing an e-mail to the DPO; • towards entities that have an international structure and which have provided for the signing, at group level, of specific Binding Corporate Rules, pursuant to art. 47 of the GDPR; | |

| | | | |
|-----------------|-----------|--------------|--------------|
| CONFIDENTIALITY | INTEGRITY | AVAILABILITY | TRACEABILITY |
| INTERNAL | MEDIUM | MEDIUM | LOW |

- if the Data Subject has given his/her explicit consent, in execution of a contract or pre-contractual measures, to ascertain or defend a right in court, to protect the vital interests of a Data Subject or of other persons and the Data Subject cannot provide his/hers consent (art. 49 of the GDPR).


| | |
|---|--|
|  | <i>RIGHTS OF DATA SUBJECTS (ARTICLES 15-22 OF THE GDPR)</i> |
|---|--|

Data Subject has the right to obtain, from the Data Controller, confirmation as to whether or not personal data concerning him or her are being processed and, consequently, to request access to personal data (art. 15 of the GDPR), rectification (art. 16 of the GDPR), cancellation (art. 17 of the GDPR) or limitation of processing (art. 18 of the GDPR), as well as to data portability (art. 20 of the GDPR).


The Data Subject has the right to object to the processing carried out on the basis of the art. 6, paragraph 1 letters e (*execution of a task of public interest or connected to the exercise of public powers*) and f (*legitimate interest*), for reasons connected to his/her particular situation (art. 21 of the GDPR).

The Data Subject also has the right not to be subjected to a decision based solely on automated processing, if it produces legal effects or if it significantly affects him/her (art. 22 of the GDPR). At any time, the Data Subject has the right to withdraw consent, without prejudice, however, to the lawfulness of the processing based on the consent given before the revocation.

Data Subject has also the right to lodge a complaint with a Supervisory Authority.

| | |
|--|-------------------------|
|  | <i>PROFILING</i> |
|--|-------------------------|

No profiling processes are implemented at the Data Controller's premises for employees, relatives and family members.

| | |
|---|--------------------------------|
|  | <i>FURTHER PURPOSES</i> |
|---|--------------------------------|

If the data controller intends to further process the personal data for a purpose other than that for which they were collected, before such further processing it undertakes to provide the interested party with information regarding this different purpose and any further relevant information.

| | | | |
|-----------------|-----------|--------------|--------------|
| CONFIDENTIALITY | INTEGRITY | AVAILABILITY | TRACEABILITY |
| INTERNAL | MEDIUM | MEDIUM | LOW |

Consensus formula

The undersigned, having acquired the information referred to in articles 13 of Regulation (EU) 2016/679, by placing his signature at the bottom of this form, declares to consent or not to consent to the processing of his personal data for the purposes indicated below:

| Purpose | Consent to Processing | |
|---|------------------------------|-----------------------------|
| <i>Training not mandatory by law</i> | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| <i>Dissemination on the website, on social media, on business cards or on the noticeboard of photos or data relating to the professional curriculum</i> | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

Date

Signature

Consent form for family members

As can be deduced from the above, in relation to the employment/collaboration relationship, the Data Controller is required to process data relating to the family members and relatives of his collaborator.

These are situations for which information is required and, if not required by law, consent to processing is required.

The data that the company processes concerns the following purposes:

- Use of permits for Law 104/92;
- Organization of events where the presence of a relative is permitted;
- Advance of severance pay;
- IBAN in case of credits (bank transfer to the family member's bank account; joint account of the bank account);
- Contact details for urgent communications;
- Tax deductions and refunds.

In relation to the above, the undersigned, _____
born on _____, relative of the collaborator _____
having acquired the information referred to in articles 13 and 14 of Regulation (EU) 2016/679, in relation to the consent to the processing of personal data, declares the following:

| Applicable | Purpose | Consent | |
|------------------------------|---|------------------------------|-----------------------------|
| Yes <input type="checkbox"/> | Use of permits L. 104/92; | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Yes <input type="checkbox"/> | Organization of activities; | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Yes <input type="checkbox"/> | Advance of severance pay | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Yes <input type="checkbox"/> | IBAN in case of credits (bank transfer to the family member's bank account; joint account of the bank account); | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Yes <input type="checkbox"/> | Contact details for urgent communications; | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Yes <input type="checkbox"/> | Tax deductions and refunds | Yes <input type="checkbox"/> | No <input type="checkbox"/> |

Date

Signature

Warning: if the relative is a minor or a person deprived in whole or in part of autonomy, consent is given signing by the person exercising parental authority or by the person who protects the data subject, reporting his/her personal details and his/her role in the following notes.

Note: