

## SUPPLIER PERSONAL DATA PROTECTION POLICY

### 1. Foreword

**Solina** pays great attention to protect the confidentiality of the personal data of its employees and suppliers and makes an ongoing effort to ensure strict compliance with personal data protection rules.

Employees and suppliers are therefore invited to carefully read this policy, the objective of which is to present how **Solina** processes their data in the context of the commercial relations and purchase/sale contracts with **Solina**.

This policy only covers data of which **Solina** is the data controller and therefore not any processing that may be established or performed outside the scope of governance specified by **Solina** (so-called 'shadow IT').

### 2. Objective of the policy

The purpose of this policy is to meet the information obligation of **Solina** under the GDPR (Article 12) and to document the rights and obligations of its customers and contacts regarding the processing of their personal data.

### 3. Legal basis and purpose of processing

Processing relating to the provision of products and services is always based on the performance of purchase/sale contracts entered into by **Solina** and its suppliers.

Processing is also always carried out for the purpose of purchasing from our suppliers the products we require for our business activities (e.g. raw materials, electronic products, etc.).

Personal data may be used for the following purposes:

| Purpose   | Comments   |
|---|--|
| <b>Administration of purchase orders, commercial contracts and services</b> | We are required to process the data of the persons we work with on a day-to-day basis in order to effectively administer commercial contracts. |
| <b>Invoicing, payment and accounts</b>                                      | We process the data of our contact persons for the invoicing and payment purposes of orders placed.  |
| <b>Order administration</b>   | We process data in order to manage our orders.   |
| <b>Access administration</b>  | We process the data of supplier's employees who access our premises, notably in order to issue access badges.                                  |
| <b>Administration of contact requests</b>                                   | We process the data of persons wishing to become one of our suppliers.   |

### 4. Data controller

**Solina** is the data controller, i.e. the person who has established the purposes and means of the processing carried out to perform the purchase/sale contracts with suppliers.

**Solina** may use the services of data processors to provide certain services (e.g. accounts). In such cases, the processor is bound by the data protection provisions of the GDPR.

It should be noted that the supplier is responsible for its own processing relating to the administration of stocks, customer orders and payments and, in more general terms, for the whole range of its activities. The supplier must therefore comply with all provisions of the GDPR, notably in relation to its employees and data processors.

Under no circumstances may **Solina** and the supplier be considered to be joint controllers within the meaning of the GDPR. There solely exists a relationship between two data controllers.

## 5. Categories and sources of data collected

Data are mainly collected directly from the contact persons of **Solina's** suppliers.

We therefore only collect and use the data required to execute the contract, namely:

- The identity of the contact persons managing an activity (e.g. surname, first names, supplier identification number);
- The business contact details of the contact persons managing an activity (e.g. business and postal addresses, business landline or mobile number, fax number);
- Professional status of the contact persons managing an activity (e.g. post, grade, function);
- Photos of the contact persons managing an activity (e.g. if they visit our premises).

## 6. Data recipients – authorisation & traceability

**Solina** ensures that the data collected and processed in the context of contracts entered into with suppliers can only be accessed by authorised internal and external recipients, notably:

| Recipient                    | Comments   |
|------------------------------|--|
| <i>Visitor reception</i>     | Reception personnel at the premises collect the data in a register of persons wishing to gain access.                      |
| <i>Relevant departments</i>  | Data is only collected internally by the personnel involved in the processing and execution of the purchase/sale contract. |
| <i>Competent authorities</i> | <b>Solina</b> may be required to share certain data with officers of the court, the police and judicial officers.          |

Recipients of the personal data of suppliers within **Solina** are bound by a confidentiality obligation.

**Solina** decides which recipients may access which data by means of an authorisation policy.

**Solina** may not be held liable for any damage that may result from any unlawful access to personal data.

All access to the processing of suppliers' personal data is traceable.

Personal data may also be forwarded to any authority legally entitled to receive it. In such cases, **Solina** is not liable for the manner in which said personnel and authorities access and exploit the data.

## 7. Retention period

The retention period of applicant data is defined by **Solina** in accordance with its legal and contractual obligations and, failing this, depending on its specific needs.

| Data category                           | Retention period   |
|---|--|
| <i>Contact persons' data</i>            | Throughout the duration of the contract extended by the contractual term of guarantees as well as the legal limitation period in the event of a dispute. |
| <i>Commercial contracts and orders</i>  | Information relating to commercial contracts and orders is retained for 10 years from the signing date of the contract.                                  |
| <i>Invoicing and payment</i>            | Information relating to invoice and payment administration is retained for 10 years.   |
| <i>Video surveillance camera images</i> | Video surveillance camera images are retained for a maximum of 1 month.  |

**Sales development data**

Data used in the context of sales development activities is retained for 3 years from the end of the commercial relationship or last time of contact.

All the stated retention periods shall be extended to the applicable legal period for evidential purposes in the event of court action. The retention period shall be extended for the duration of the court action, as applicable.

After the specified periods, data is either deleted or retained after anonymization, notably for statistical purposes.

Suppliers are reminded that deletion or anonymization are irreversible operations and data cannot be subsequently restored by **Solina**.

**8. Confirmation and access right**

The suppliers' employees enjoy the right to request confirmation of whether or not **Solina** is actually processing their personal data within the framework of the purchase/sale contract.

The suppliers' employees may also request **Solina** to provide a copy of their data being processed.

However, in the event of a request for additional copies, **Solina** may ask the suppliers' personnel to cover the associated costs.

If the suppliers' personnel request a copy of their personal data via electronic means, the requested information will be provided in a commonly used electronic format, unless specified otherwise.

The suppliers' employees are notified that this access right may not cover confidential information or data, or data for which communication is prohibited by law.

The access right may not be exercised in an abusive manner, i.e. exercised legally yet with the sole objective of undermining the proper execution of the services performed by **Solina**.

**9. Right to object**

Under no circumstances does **Solina** perform any sales development or profiling activities affecting suppliers' employees, who therefore do not enjoy any right to object to processing performed in the context of purchase/sale contracts entered into by **Solina** and its suppliers.

**10. Right to deletion**

The suppliers' employees may only exercise their deletion right once the contract has been terminated and no longer produces any effects on **Solina** and its suppliers.

**11. Exercise of data subjects' rights**

In order to exercise their rights, the suppliers' employees must contact **Solina** in writing, via post or e-mail at the following addresses:

**Department of Solina**

Postal address: Solina Group Holding – 13 rue de Marivaux, 75002 PARIS

Please note that the data subject alone may exercise the rights set out above.

The request must therefore be accompanied by a copy of a valid identity document. Failing this, the request will be rejected.

**Solina** makes every effort to respond to requests within a reasonable period, where possible within one month of receiving any such request.

However, should answering the request prove to be complex, or should **Solina** have a high volume of requests to be dealt with at the same time, the response period may be extended to two months.

**12. Data processors**

**Solina** notifies its suppliers that it may engage any processor of its choice to process their personal data.

In any such case, **Solina** ensures that the processor complies with its obligations under the GDPR.

**Solina** undertakes to sign a contract with all processors imposing on the latter the same data protection obligations that apply to the Entity. Furthermore, **Solina** reserves the right to perform an audit on the processor to verify the latter's compliance with its obligations under the GDPR.

### 13. Security

**Solina** is required to implement security techniques of a physical or logical nature which it judges to be appropriate to prevent the destruction, loss, degradation or unauthorised disclosure of data in an accidental or illegal manner.

The main elements of these measures are:

- Management of data access rights;
- Internal back-up;
- Identification processes;
- Security audits;
- Implementation of an IT system security policy;
- Implementation of business continuity and disaster recovery plans;
- Utilisation of security protocols and/or solutions.

### 14. Data breach

**Solina** undertakes to notify to the authority any data breach it may incur, in accordance with the conditions set out in personal data regulations.

The suppliers' employees are notified of any data breach that may constitute a high level or risk to their privacy.

### 15. Data Protection Officer

**Solina** has designated a Data Protection Officer who may be contacted for any questions relating to the processing carried out by **Solina**:

**Data Protection Officer**

Name: Racine

E-mail address: dpo-solina@racine.eu

### 16. Processing record

As data controller, **Solina** undertakes to maintain a register recording all completed processing activities.

This register is a document or app that lists all processing carried out by **Solina** in its capacity as data controller.

**Solina** undertakes to provide any supervisory authority on request with all information enabling said authority to verify the compliance of processing with applicable data protection regulations.

### 17. Right to submit a complaint to the authority

The suppliers' employees enjoy the right to submit a complaint to a supervisory authority, i.e. CNIL in France, should they believe that the processing of their personal data does not comply with EU data protection regulations, at the following address:

**CNIL**

3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07, FRANCE

+33 (0)1 53 73 22 22



**18. For further information**

For any further general information about personal data protection, please consult the authority website at [cnil.fr](https://cnil.fr).