Customer and contacts personal data protection policy

1. Foreword

Regulation (EU) 2016/679 of the European Parliament and of the Council dated of the 27th of April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data, otherwise known as the General Data Protection Regulation (GDPR) sets out the legal framework for the processing of personal data.

The GDPR strengthens the rights and obligations of data controllers, processors, data subjects and data recipients.

We process personal data during the course of our business activities.

Please note the following definitions of certain terms used in this policy:

- Data controller: SOLINA GROUP SERVICES, (hereafter the "Entity");
- Data processor: natural person or legal entity who processes personal data on behalf of the Organisation;
- Data subject: customers and/or contacts of the Entity;
- Data recipient: a natural person or legal entity who receive personal data from the Entity. Data recipients may therefore also be employees of the Entity or of external entities (partners, exhibitors, banks, service providers, etc.).

In Article 12, the GDPR requires that data subjects are notified of their rights in a concise, transparent, comprehensible and easily accessible manner.

2. Purpose

The purpose of this policy is to meet the information obligation of the Entity 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. Scope

This policy applies to all processing of the personal data of the Entity's customers and contacts.

The Entity makes every effort to ensure that said data is processed within the framework of strict internal governance. That being said, this policy only covers data of which the Entity is the data controller and therefore not any processing that may be established or performed outside the scope of governance specified by the Entity (so-called 'shadow IT').

The processing of personal data may be managed directly by the Entity or via a data processor specifically designated by the Entity.

This policy is independent of any other document that may apply in the context of the contractual relationship between the Entity and its customers or contacts.

4. Types of data collected

Non-technical data ***(depending on the circumstances)***	• Identity and identification (surname, first name, date of birth, pseudonym, customer number) • Contact details (e-mail, postal address, phone number): notably for sending newsletters • Professional activities, if applicable (company name, function) • Bank details, if required • Data relating to current contracts
Technical data (if applicable)	• Identification or connection data such as IP address or logs

5. Data sources

Data related to our customers and contacts are generally collected from them directly (direct collection).

Collection may also be indirect via specialist companies or partners and suppliers of the Entity. In such cases, the Entity takes the greatest of care to ensure the quality of data it receives.

6. Purposes and legal bases

The Entity processes your data for the following purposes, as applicable:

- Customer relationship management (CRM);
- Prospect relationship management (PRM);
- Organising events;
- Purchasing administration;
- Business monitoring;
- Newsletter administration;
- Improving services and satisfaction surveys;
- Targeted advertising and segmentation;
- Mobile app administration;
- Statistics.

These purposes are based on the execution of the contract or the legitimate interests of the Entity to hold data concerning its users and contacts.

The Entity's relationships with its customers will be based on the general terms and conditions of sale, duly accepted on registration.

7. Data recipients – authorisation & traceability

The Entity ensures that data can only be accessed by authorised internal and external recipients.

Internal recipients	External recipients
- Authorised personnel from Marketing, departments responsible for managing the customer relationship and sales development, Communications, Sales, IT and their line managers; - Authorised personnel from departments responsible for control and audit functions (departments responsible for internal control procedures, etc.);	- Partners, external companies and subsidiaries of a single group of companies; - Organisations, officers of the court and judicial officers in the context of their debt collection functions; - The body responsible for managing the list of cold-calling prohibitions; - Data processors' authorised personnel.

Recipients within the Entity of the personal data of customers and contacts are bound by a confidentiality obligation.

The Entity decides which recipients may access which data by means of an authorisation policy.

All access to the processing of customers' and contacts' personal data is traceable.

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

8. Retention period

The retention period of applicant data is defined by the Entity in accordance with its legal and contractual obligations and, failing this, depending on the specific needs, notably in accordance with the following principles:

Processing	Retention period
Customer data	For the duration of contractual relations with the Entity, plus 5 years for sales development purposes, without prejudice to storage and retention obligations or the statute of limitations
Data relating to contacts and potential customers	3 years from collection of the data by the Entity or from the last contact made by the potential customer or contact
Bank details	Deleted on expiry of the master agreement If a transaction is disputed: 13 months' retention in the files following the data of debit

After the specified periods, data is either deleted or retained after anonymization, notably for statistical purposes. It may be retained in the event of pre-litigation and litigation.

Customers and contacts are reminded that deletion or anonymization are irreversible operations and data cannot be subsequently restored by the Entity.

9. Confirmation and access right

Customers and contacts are entitled to request the Entity to issue confirmation of whether or not their personal data is being processed.

Customers and contacts also enjoy an access right, subject to compliance with the following rules:

- The request is issued personally and is accompanied by a valid identity document;

- It is issued in writing to the following address: dpo@solina.com

Customers and contacts are entitled to request a copy of their personal data being processed by the Entity. However, in the event of any additional copies being requested, the Entity may require the customer or contact to cover the associated costs.

If customers or contacts 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.

Customers and contacts 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 service in question.

10. Updating and rectification

The Entity will meet updating requests:

- Automatically, for online modifications relating to fields that may be updated technically or legally;
- On written request, issued by the data subject personally on proof of identity.

11. Right to deletion

The deletion right of customers and contacts does not apply where processing is carried out in compliance with a legal obligation.

In other circumstances, customers and contacts may request deletion of their data if any of the following criteria are met:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- If the data subject withdraws the consent on which the processing has been based and it exists no other legal basis;

- The data subject objects to processing required for the Entity to pursue its legitimate interests and there exists no other pressing and legitimate reason to continue processing;
- The data subject objects to the processing of their personal data for marketing purposes, including profiling;
- The personal data has been processed unlawfully.

In accordance with legislation of personal data protection, customers and contacts are notified that this is an individual right that may only be exercised by the data subject in relation to their own information: for security reasons, the department concerned must therefore verify your identity before communicating any of your confidential information to a person other than you.

12. Right to restrict processing

Customers and contacts are notified that the right to restrict processing is not intended to apply when the processing carried out by the Entity is legal and all the personal data collected are necessary for performance of its services.

13. Data portability right

The Entity will accede to data portability requests in the specific circumstances of data communicated by customers and contacts personally, via online services provided by the Entity itself and for purposes based solely on personal consent. In such cases, the data will be communicated in structured and commonly used format able to be read by a machine.

14. Automated individual decision-making

The Entity does not carry out automated individual decision-making.

15. Optional or mandatory nature of responses

Customers and contacts are notified on every personal data collection form of the mandatory or optional nature of responses by means of an asterisk.

If a response is mandatory, the Entity explains the consequences of non-response to customers and contacts.

16. Right of use

The Entity is assigned by customers and contacts a right to use and process their personal data for the aforementioned purposes.

However, any data supplemented by the processing and analysis of the Entity, otherwise known as supplemented data, shall remain the exclusive property of the Entity (usage analysis, statistics, etc.).

17. Data processors

The Entity notifies its customers and contacts that it may engage any processor of its choice to process their personal data.

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

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

18. Security

The Entity 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.

19. Data breach

In the event of any breach of personal data, the Entity undertakes to notify the authority as set out in the GDPR.

Should any such breach present a high level of risk for customers and contacts and the data has not been protected, the Entity shall:

- Notify the customers and contacts concerned;
- Issue the necessary information and recommendations to the customers and contacts concerned.

20. Data Protection Officer

The Entity has designated a Data Protection Officer.

The contact details of the Data Protection Officer are as follows:

- Name: **Racine Law Firm**
- E-mail address: dpo@solina.com

If personal data is to be subjected to additional processing, the Entity will notify the Data Protection Officer in advance.

Should customers and contacts wish to obtain any particular information or pose a specific question, they may contact the Data Protection Officer who will provide a

response within a reasonable period in light of the question posed or information requested.

In the event of encountering any problem with the processing of personal data, customers and contacts may contact the designated Data Protection Officer.

21. Processing record

As data controller, the Entity undertakes to maintain a register recording all completed processing activities, if the law requires it.

This record is a document or app that lists all processing carried out by the Entity in its capacity as data controller.

The Entity 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.

22. Right to submit a complaint to the authority

Customers and contacts concerned by the processing of their personal data 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

+33 (0)1 53 73 22 22

23. Regulatory developments

This policy may be amended or supplemented at any time in the event of legal or judicial developments, or in response to new uses and any decisions or recommendations issued by the authority.

Any new version of this policy will be notified to customers and contacts via all reasonable means defined by the Entity, including electronically (e.g. notification via e-mail or online).

24. For further information

For any further general information about personal data protection, please consult the authority website at cnil.fr.