RINA GROUP

BINDING CORPORATE RULES SUMMARY

(according to European General Data Protection Regulation 2016/679)

Binding Corporate Rules (BCRs) are aimed to allow multinational companies to transfer personal data to their affiliates located outside of the European Union. Binding Corporate Rules define, within the organization of RINA Group, how to deal with data protection regulation requirements, with specific reference to transfer of personal data between all the companies belonging to the Group.

According to what stated in *Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)* adopted by the EDPB on 20 June 2023, RINA S.p.A. draws up this document.

Reference to this document is available at the Privacy Notices provided for data subjects pursuant to Article 13 GDPR and on the company's website.

RINA S.p.A. provides for following information in full and by a clear and plain language; RINA S.p.A. promptly updates such document in case of any changes.

1. Material scope of application

The processing and data transfer among the RINA Group companies are made for the following purposes:

- Database management
- Business development
- Employee recruitment
- Employee administration
- Training
- Execution of contracts with clients
- Execution of contracts with suppliers
- Marketing, sales and promotions
- Finance and accounting
- Legal affairs management
- Merger and acquisition operations
- Internal management and audit

With reference to the above, the following kind of Data Subject can be identified:

- Customers

- Employees and their relatives
- Suppliers
- Non-exclusive personnel
- Other individuals (i.e., business partners)

RINA Group companies process personal data through collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of

- personal data
- special categories of personal data
- personal data relating to criminal convictions and offences.

2. Definitions and, if applicable, list of abbreviations

Definitions

"**Binding corporate rules (BCR) or rules**": personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

"**Controller**": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"**BCR Lead**": the Italian Supervisory Authority, Garante per la protezione dei dati personali.

"**Competent Supervisory Authority" or** "**SAs**": pursuant to Article 51 GDPR, authority competent to assess the respect of the BCR by the data importer in the third country in relation to the relevant transfers and by the data exporter(s) of the specific transfer.

"**European Economic Area (EEA)**": consists of the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway; excluding Switzerland).

"**Personal data breach (or data breach)**": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**Data exporter**": the Data controller or Data processor within the EEA who transfers personal data to a controller or processor in a third country.

"**Data importer**": the Data controller or Data processor located in a third country that receives personal data from the Data exporter.

"**Data protection officer (DPO)**": an expert who assists an organisation with internal compliance, information and advice on data protection obligations and acts as a contact point for data subjects and the supervisory authority.

"**Data subject**": the physical person to whom the personal data refer.

"**Organizational measures**": internal policies, organisational methods or standards, and controls and audits, that controllers and processors can apply to ensure the security of personal data.

"**Personal data**": any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Processing**": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**": a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"**Records of processing activities**": logs of a business or website's data processing activities. Those logs include data categories, groups of data subjects, purposes of the processing, and data recipients.

"**Security measures**": set of all technical and organizational arrangements used to ensure that data are not destroyed or lost even accidentally, as well as access to data to authorized persons only.

"**Liable BCR Member**": BCR Member established on the territory of an EEA Member State, that is responsible for any violation of the adopted BCR by other Group Companies located in non-EEA countries. To this end, the Liable BCR Member is RINA S.p.A.

"**BCR Members**": RINA Group Companies bound by these BCR within the framework of the Group Regulation – *Exercise of management and coordination* and intra-group stipulated contracts.

"**BCR Contact**": natural person identified by each RINA Group Company with the responsibility of making effective the BCR system as defined below. The BCR Contact acts as an intermediary between RINA S.p.A. and the local companies.

"**Technical measures**": measures that can be implemented physically, such as alert systems, firewalls and pseudonymisation of personal data.

"**Third party**": any physical or legal person, public authority, agency, or any other body other than the data subject, the Data Controller, the Data Processor, and persons who, under the direct authority of the Data Controller or the Data Processor, are authorized to process the personal data of the Data Subject.

Abbreviations

GDPR: General Data Protection Regulation

BCR: Binding Corporate Rules

EEA: European Economic Agreement

EU: European Union

DPO: Data Protection Officer

EDPB: European Data Protection Board

WP: Working Party

S.p.A.: Società per Azioni

SA: Supervisory Authority

DPIA: Data Protection Impact Assessment

ESG: Environmental, Social and Governance

IA: Internal Audit

BoD: Boards of Directors

CEO: Chief Executive Officer

OU: Organizational Units

CB: Control Body

3. Clauses related to Group's liability within the BCR

RINA S.p.A shall be the solely responsible for any violation of the BCR (*i.e.,* Liable BCR Member).

It also agrees to take as its responsibility the charge to adopt the necessary actions to remedy the acts of other members outside of the EEA bound by the BCR and to pay compensation for any material or non-material damages resulting from the violation of the BCR by Group members.

In any case, if a RINA company outside the EEA violates the BCR, the competent Authority or other judicial authorities will be in the EU and Data Subjects will have the rights and remedies against RINA S.p.A, as Group member that has accepted responsibility and liability arising from the violation as if it had been caused by it in Italy, instead of the BCR member outside di EEA.

Please note that RINA S.p.A will discharge itself from any responsibility, if it proves that the Group member outside the EEA is not liable for any violation of the rules which has resulted in the Data Subject claiming damages, or that no such breach tooks place.

Liable BCR member (RINA S.p.A.) has sufficient assets or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the BCR. Such confirmation is renewed at the occasion of every annual update.

4. Clauses relating to the data protection principles, to the lawfulness of the processing, to security and personal data breach notifications, to restrictions on onward transfers

All RINA Group personnel will process personal data according to the following principles.

a) Lawfulness, fairness, and transparency

Personal data will be processed in a lawful, fairly and transparent manner, according to the GDPR provisions.

Transparent information is given to Data Subjects about the data processing that will be done by providing, at the time when their data are collected, the information prescribes by artt. 13 and 14 GDPR, in a clear and comprehensive manner, through privacy policy or other privacy notices.

b) Processing special categories of personal data

Data belonging to special categories according to art. 9 GDPR will be process only if one of the criteria included in Article GDPR applies. The most commonly used are:

- the Data Subject has given his/her explicit consent.

- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the RINA Group Company or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorized by EU, Member State or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.
- the Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.
- the Processing is otherwise permitted under the GDPR or the applicable law of the country of establishment of the Entity.

c) Purpose limitations

Personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Data can only be collected for specific processing purposes that the subject has been made aware of and no other, without further consent.

Each Company of the Group is bound to pre-define the purposes of any processing carried out and to make them explicit from the moment that the data is collected, within the information given to the Data Subject and in the dedicated section of the Record referred to in art. 30 GDPR.

Furthermore, in the case of a new purpose, each Company will substantially and not merely formally assess the compatibility of the further purpose with the one for which the data was collected. In cases where the new data processing may not be reconducted to purposes prior identified, it is necessary to give an integrated privacy notice pursuant to Article 13 GDPR.

d) Data minimization

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; no more than the minimum amount of data is kept for specific processing.

The processing will not be carried out in all cases where the same purposes can be achieved by means of anonymous data or other methods that make it impossible to determine the identity of the Data Subject.

In addition, each Company defines and formalizes different levels of authorization for each person involved in the processing of data, so as to ensure that each person formally authorized to process data only accesses the categories of data that are essential for the performance of his/her job.

e) Accuracy

Personal data must be accurate and, where necessary, kept up to date. If group companies become aware that the personal data it has transferred or received is inaccurate, or has become outdated, they shall inform the DPO that may involve such companies without undue delay.

In order to keep the personal data accurate and up-to-date, RINA Group companies have put in place internal processes encouraging the Data Subjects to inform them whenever their data are modified or needs to be updated and have adopted tools that permit to up-to-date periodically certain categories of data.

f) Storage limitations

Personal data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data no longer required for processing should be removed or stored with strongly limited access to them, in order to allow Data Controller to exercise or defend a legal claim.

g) Integrity and confidentiality

Personal data must be processed in a manner that ensures their security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

h) Security

RINA Group implements appropriate technical and organizational measures to protect personal data from unauthorized use, disclosure, destruction and alteration.

Each RINA Company implements an articulated privacy risk management system: identifying the risks associated with the processing; evaluating these risks in terms of origin, nature, probability and severity; defining best practices to mitigate the risk associated with each processing performed.

The adequacy of the measures adopted for each processing operation shall be assessed ex ante, from a preventive perspective, and ex post, following any changes in reference context.

i) Data Processor

Each company shall stipulate an agreement under art. 28 GDPR with all its sub processors/processors, which includes all the requirements of Art. 28, par. 3 GDPR. RINA Group has adopted a Data Processing Agreement template, examined also by the DPO and made available to all Group Companies. In cases where other contractual parties provide for

a template, Group Companies should assess the content of such document and ask for a DPO's advice.

j) Data breach

The information about data Breach or other conducts or events that may lead to a violation of the Model or that, more generally, are relevant for the purposes of the Privacy legislation must be transmitted preferably in writing, to the DPO e to the Liable BCR Member (RINA S.p.A.).

In addition, RINA Group has adopted a procedure to manage potentially breach in which is formalized the duty to notify without undue delay and, not later than 72 hours, any personal data breaches to the Authority and the data subject when necessary (i.e. where the personal data breach is likely to result in a high risk to their rights and freedoms in line with the requirements of Article 34 GDPR).

k) Data transfer outside the Group

Personal data shall be transferred outside the Group to data controller/processor/sub processor only when applies one of the measures provided by artt.45-49 GDPR.

In the event that one of the Companies of the Group transfers personal data to a third party which is not a member of the RINA Group, and which is located in a non-EEA country, as these transfers will not be covered by these BCR, the Company is obliged to take the steps described in Chapter V.

l) Data transfers in and outside RINA Group to countries that do not guarantee the same level of protection of the EU one

With reference to data transfer to countries that do not guarantee the same level of protection as the GDPR, RINa Group has defined a set of supplementary security measures to be adopted.

Group companies carry out regular checks to ensure that those measures continue to provide an appropriate level of security.

5. Clauses relating to the rights of data subjects

Any Data Subject has fundamental rights relevant to his/her personal data processing:

- **The right to access to his/her personal data processed by RINA Group companies:** The data subject shall have the right to obtain from the BCR Member confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. Data subject has also the right to have the following information:
    - the purposes of the processing;

- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22, par. 1 and 4 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

In addition, where personal data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

- **The right to have inaccurate or incomplete personal data to be corrected, updated, deleted, or blocked:** the Data Subject shall have the right to obtain from the Data Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **The right to erasure ('right to be forgotten'):** the so-called "to be forgotten" right refers to the erasure of personal data in a strengthened form. In fact, it is envisaged the obligation for the Controller (if they have "disclosed to the public" the personal data of the data subject for example, posting them on a website) to inform of the cancellation request also co-controllers or external processors who process the deleted personal data, including "any link, copy or reproduction".
- **The right to request not to be subject to a decision based solely on automated processing, including profiling, which produces legal effect on him/her or significantly affect him/her**: the Data Subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic

refusal of an online credit application or e-recruiting practices without any human intervention.

However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the Data controller, or necessary for the entering or performance of a contract between the Data Subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

- **The right to data portability**: where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one Data Subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with GDPR. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in GDPR and should, in particular, not imply the erasure of personal data concerning the Data Subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract.

Where technically feasible, the Data Subject should have the right to have the personal data transmitted directly from one controller to another.

- **The right to restrict the data processing in case of unlawful processing:** it can be exercised not only in case of violation of the conditions of lawfulness of the processing (as an alternative to the cancellation of the data themselves), but also if the data subject requests data correction (pending the amendment by the Controller) or opposes to the processing pursuant to art. 21 of the Regulation (pending the evaluation by the Controller). Excluding the storage, any other processing of the data whose limitation is requested is prohibited unless certain circumstances occur (consent of the interested party, assessment of rights in court, protection of rights of another natural or legal person, significant public interest).
- **The right to complain before the competent Supervisory Authority (choice between the Authority in the Member State of his habitual residence, place of work or place of the alleged infringement) and before the competent court of the EU Member States (choice for the data subject to act before the courts where the controller or processor has an establishment or where the data subject has his or her habitual residence):** every Data Subject should have the right to lodge a complaint before the competent court of the EU Member States as well as before a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter of Fundamental Rights of the European Union if the data subject considers that his or her rights under GDPR are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.
- **The right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR:** where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives

which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects.

6. Steps to lodge a complaint with a SA or before the competent Court

Data subjects have rights to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR. The BCR members accept that data subjects may be represented by a non-profit body, organisation or association, under conditions set out in Article 80 GDPR.

As described above, data subjects have the right to lodge a complaint:

- With a Supervisory Authority, in particular in the Member State of the data subjects' habitual residence, place of work or place of the alleged infringement; and
- Before the competent court of the Member States where the controller or the processor has an establishment, or where the data subject has their habitual residence.

It should be pointed out that the rights listed above do not extend to those elements of the BCR pertaining to internal mechanisms implemented within entities such as detail of training, audit programmes, compliance network and mechanism for updating of the BCR.

7. Steps to lodge any complaint with BCR Members related to the processing of their personal data as well as point of contacts which address the compliant to

If any Data Subject has doubts, questions, or complaint regarding the compliance of the data processing to the Rules, he/she can contact RINA Data Protection Officer (rina.dpo@rina.org or to the postal address: Via Corsica 12, 16128 - Genova), or can send a whistleblowing report, also in complete anonymity, via a voice channel or a web platform, both accessible from the RINA website: https://www.rina.org/it/about-us/whistleblowing-reports .The DPO will answer to the questions and try to solve the issue.

In the event that complaints should reach the Companies of the RINA Group through other channels, the BCR Contact is required to forward what is received immediately to the above address. It is understood that, in order to facilitate the Data Subject, RINA Group also accepts complaints that are not submitted using the contacts indicated above, provided that they are properly substantiated. Any deficiencies that preclude the correct assessment of the request/complaint received will be remedied by the DPO through requests to the Data Subject.

Anyway, when receiving a complaint, the DPO, with BCR Contacts' support, will take charge of every complaint received by providing:

- record the complaint in a specific register,
- verify the identity of the Data Subject and the legitimacy of the request,
- assess the complexity of the complaint/request and if it is not possible to respond within one month notify the Data Subject,
- find the complaint/request within one month or at most 3 months in case of complexity,
- inform the Data Subject of the possible extension of the time of feedback and the reasons for it,
- in case of justified complaints, involve the relevant departments of the RINA Group Companies concerned in order to define the action to be taken following the complaint/request,
- progressively inform the Data Subject about the various stages of receiving and handling the complaint/request,
- in case of rejection of the complaint, inform the Data Subject of the reasons on which it is based and of the actionable instruments against such decision,
- if the complaint is upheld, inform the Data Subject of the reasons for this assessment, the action taken as a result of it and any protective measures that may be taken.

To each of the requests regarding the compliance to the BCR the DPO must always give a motivated answer (even in case of denial) to the claimant Data Subject, cooperating with him to solve the issue or to reach an agreement.

Finally, if Data Subject is not satisfied by the solution proposed, he/she can:

i. Lodge a complaint before the Data Protection Authority. See par. **Errore. L'origine riferimento non è stata trovata.**.
ii. Lodge a claim before a competent court (of the EU State where he/she resides or work or where the alleged breach occurred). See par. **Errore. L'origine riferimento non è stata trovata.**.

Please also note that if the Data Subject believes that his/her personal data has been processed unlawfully, inappropriately or in any case not in accordance with the provisions of the aforementioned Binding Corporate Rules, he/she may also lodge a complaint:

- to the relevant Data Protection Authority which will be or the Data Protection Authority in the Regulated Jurisdiction of his habitual place of residence when the Personal Data concerned by the complaint or the place of the alleged violation have been acquired and
- to the competent jurisdictions of an EEA country at the choice of the Data Subject: the Data Subject may choose to take legal action before the judicial authorities of the EEA country in which the Data Exporter is established or before the judicial authorities of the EEA country in which the Data Subject had his or her habitual

residence at the time of acquisition of the Personal Data concerned by the complaint.

The right to lodge a claim before the competent court and a complaint before a SA is not dependent on the data subject having used the internal complaint handling process beforehand.

Data Subject may also ask to the competent Court for compensation in the event of an alleged breach of the Rules.

8. BCR members' contacts (*i.e.*, address, number of company registration, etc.).

Contact details of the legal entities in each Country can be found on the website at the following https://www.rina.org/en/contacts.