PRIVACY DATA GOVERNANCE

IT Security Policy and privacy and data and information security

All the professionals at SCM handle a significant amount of information and personal details concerning employees, clients and third parties. The essence of the Group's work consists of handling legal, contractual, business and client-related data so, as a result, data protection is one of the profiles which the Group places a lot of weight on in order to comply with European and international standards.
Data protection is a priority for the Group all over the world, set out as part of its *governance* and *business* model because it can have positive consequences for safeguarding the brand, reducing operating losses, the quality of client relations, the level of trust with all the parties concerned and compliance with legal obligations.

The Group has adopted organisational and operational measures and expedients to protect any individual who enters into relations with the Group's *entities*. SCM Group has introduced an extensive personal data protection programme which will be set out in the sections below, representative of the programme's distinctive features.

1. Organisational and operational measures and expedients aimed at protecting personal data suitable for identifying those involved.

2. IT Security Policy technical measures and expedients aimed at appeasing the risks threatening the processed personal data.

Data Protection Compliance Programme

SCM Group is committed to protecting the personal data it processes with an approach based on risk evaluation, intrinsic to each processing, coherent with the applicable legal requirements and with employee, client and third-party expectations, as well as all those who come into contact with the Group for whatever reason.
SCM Group is keen to improve its personal data protection system, with a view to satisfying the requests from clients and the requirements of current legislation such as EU Reg. EU 2016/679 concerning personal data protection and the EDPB guidelines. In that way, with a view to respecting the principle of accountability, the Group has identified and adopted technical and organisational measures aimed at reinforcing the protection of processed personal data and of appeasing any risks.
The Group has also established a *Privacy Committee* where problems which emerge from the application of the legal protocol are analysed and resolved. The *data protection* programme is arranged into different levels of organisation: at Global level, at Member Firm level and at individual country level.

GDPR

The General Data Protection Regulation, officially Regulation no. 2016/679 and known by its initials GDPR, which came into force in April 2016 and became effective as of 25 May 2018, has made significant changes to the legislation governing data protection in Europe. The Regulation is aimed at standardising the laws surrounding processing and protection of information between Member States in the European Union, guaranteeing individuals (including all those with relations with clients and Group employees) greater control rights over their own personal data.
The data collected, the privacy and the risk to safety are topics covered at global level and which SCM Group holds as priority.
The most advanced countries in the world, with multinational, dynamic markets, have tools, procedures and legislation elevating the GDPR to «gold standard». The organisations are responsible for adopting adequate personal data protection measures based on the actual and current risks

threatening their data. The Group has tried to draw up and implement a *Data Protection Compliance Programme* in relation to the numerous areas covered by the above-mentioned Regulation. As part of this programme, specific technical and organisational measures have been drawn up and implemented which aim to satisfy clients' applicable legal requirements and obligations. The Data Protection Compliance Programme is kept up to date to keep track of the legal development and *business* context, risk scenario and emerging technologies. The main components of SCM Group's Data Protection Compliance Programme are:

• Processing activities register – the Group has mapped out all the processing work which involves personal data, in order to correctly allocate roles and responsibilities, analyse the risks to the fundamental rights and freedoms of those involved and guarantee an effective implementation.

• Data Protection Organisational Model – the effectiveness of the protection measures depends on an adequate organisational model of the roles proposed to the management body of the operations carried out on the personal data, surveillance positions (like the *Data Protection Officer*) and warranty positions. SCM Group keeps its own benchmark organisational model up to date and has appointed its *Data Protection Officer*, keeping an all-round control of the flow of personal data circulating in other *legal entities*. The Group has introduced a discussion procedure between the appointed DPO and the other surveillance and control bodies, assessing the different links in the compliance organisational chart and advising on the possibility of capillary and widespread checks.

• Information concerning data protection – all the documentation to guarantee the Group's processing transparency has been updated to meet the GDPR requirements, in order to provide full protection to the parties in question and have full awareness of the aims, means and juridical grounds of the processing work carried out, all other necessary information and how to exercise their rights.

• Contractual clauses with third parties – SCM Group has drawn up and implemented adequate contractual clauses with all third parties with whom they have business relations both within and outside of Europe.

• Risk analysis and impact assessment (DPIA) – SCM Group in Italy has developed and adopted a new risk analysis and impact assessment to be applied, even internationally, to the data processing contained in the register, for the purpose of further identifying protection measures, with regard to the potential material and immaterial damage which data processing can incur for the parties in question.

• Policies & Procedures – implementation of new policies and procedures concerning data protection, for the purpose of meeting the requirements and standards established by the GDPR and other relevant laws, including:
- General data protection policy: Privacy Data Governance;
- Procedure for managing security violations and relative register: Data Breach procedure;
- Procedure for managing the rights of those whose data is being processed: Procedure for exercising personal data rights by the party in question (DSAR) (Data subject access requests);

• IT Security Policy – From a security point of view, SCM Group has defined rules and adopted a pervading and robust programme for the use of IT tools for the purpose of keeping company and personal data intact, private and available and protect it from IT risks.

• Employee training – All of SCM Group's employees receive information on new legislation surrounding personal data protection and are obliged to attend training courses to improve their knowledge of the risks and current legislation on matters of personal data protection.

Data Protection Officer

SCM Group s.p.a. appointed a Data Protection Officer whose role is also to control the Privacy managers of the individual legal entities which are part of the Group and with whom they interact to guarantee proper data-flow monitoring. The Data Protection Officer's role is to monitor the functioning of the technical and organisational measures adopted. They also play an informative and consulting role for all the corporate individuals proposed for data processing and management and, lastly, they act as a benchmark for the Data Protection Authority and for those whose data is being processed. The Data Protection Officer periodically informs the administrative bodies about the risk level of data protection exposure.

During the period of reporting, SCM Group's Data Protection Officer carried out monitoring work which is summed up in an annual report. This is aimed at assessing the adequacy, state of implementation and operational effectiveness of the protections and measures. The results of this check were brought to the attention of the company's control and management bodies, encouraging the consolidation of the continuous improvement plan of the data protection system. In order to guarantee improved effectiveness of the Group's Data Protection Officer's action, during the reporting period, a *data protection control framework* was established which includes the key control activities subject to periodical monitoring in order to activate IT flows which can capture all the risk dimensions for all the processed data in the personal data processing register.