Data Transfer Abroad

In some cases of data transfer to cloud suppliers based outside the EU, these suppliers are subject to the regulatory powers of local public authorities and in some situations, based on foreign legislation, (in the USA: the Federal Trade Commission, Article 702 of the FISA and the Executive Order EO 12333) the importer may be obliged to communicate the personal data transferred, in response to requests received from public authorities, to meet national security requirements (e.g. anti-terrorism) or application of local law (with consequent possible access to data, of which the importer, based on local legislation, may not have to give notice to the exporter and the interested party, who will therefore not be able to exercise the relative rights normally recognized by the GDPR).

Therefore, in the abstract, the risk cannot be excluded that in certain and exceptional situations related to the aforementioned specific requirements, the foreign public authority may process such data without applying substantially equivalent safeguards to those provided for by the GDPR to the data subject. However, the risk that the American public authority actually has an interest in applying local legislation to the transferred data appears to be reasonably negligible based on the following circumstances:

i) the performance of the exporter (IEG) in favor of the interested parties whose data the importer processes and the consequent data processing, have a limited object (the provision of exhibition services) and a limited purpose (the management of technical processes - organizational functional to the aforementioned services and the fulfillment of legal obligations); the performance does not involve the publication of personal opinions, comments or similar information, nor the making available of services or products that can be used in activities against national security;

ii) the types of personal data transferred are limited (eg personal, contact, contractual, administrative data); no particular categories of data are transferred (e.g. on political and religious opinions, biometrics); the categories of interested parties to which the data refer are limited (exhibitors, visitors, participants in events, buyers, journalists, speakers) and they concern operators belonging to product or economic categories that are not reasonably relevant with regard to national security purposes (eg tourism, wellness, machine handling, sports activities, and so on).

Therefore, IEG believes that the CCS applied in the relationship with importers (in particular the USA) effectively guarantee protection of the rights of interested parties substantially similar to that provided for by the GDPR, regardless of the application of any additional measures to the processing in question.

The adoption of additional contractual measures by IEG towards importers (e.g. obligations to communicate public access, the right to suspend or terminate the transfer and to terminate the contract with the importer, and the like), may be introduced in at any time by the exporter following any information provided to operators by the EDPB - European Data Protection Board following the judgment of the Court of Justice of the European Communities (ECJ of 17 July 2020 which declared the bilateral agreement called "Privacy Shield").

The transfer of data to the non-EU country takes place in any case also because it is necessary for the execution of i) a contract concluded between the interested party and IEG and / or pre-contractual measures adopted at the request of the interested party, or ii) of a contract stipulated between IEG and another natural or legal person (e.g. our subsidiary, supplier, with headquarters outside the EU, etc.) in favor of the interested party.