Deliberation 2022-113 of November 17, 2022 National Commission for Computing and Liberties Nature of the deliberation: Other authorization Legal status: In force Date of publication on Légifrance: Wednesday December 14, 2022 Deliberation No. 2022-113 of November 17, 2022 approving the rules of binding companies (BCR) "subcontractor" of the LEYTON group (Request for approval n°19016803)

The National Commission for Computing and Freedoms,Seizure by Thésée in the name and on behalf of the Leyton group, on September 16, 2019, of a request for approval from its subcontractor BCRs;Given the regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general regulations on data protection or GDPR), in particular its articles 47, 57 and 64; Having regard to law n ° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms; Having regard to decree n ° 2019-536 of May 29, 2019 amended taken for the application of law n ° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 73; On the proposal of Mrs. Anne DEBET , Commissioner, and after having heard the observations of Mr. Benjamin TOUZANNE, Government Commissioner, Makes the following observations: Article 47-1 of the GDPR provides that the CNIL approves Binding Corporate Rules (BCR) provided that those they meet the requirements of this article. The implementation and adoption of BCR by a group of companies aims to provide guarantees to data controllers and processors established on the territory of the European Union (EU) so that a uniform level of protection is applied to data transferred to third countries, independently of the level of protection conferred by each of these third countries. However, before applying these BCRs, it is the responsibility of the data exporter located in a Member State, if necessary in collaboration with the data importer, to assess whether the level of protection required by the law of the European Economic Area (EEA) is respected in the third country of destination, including in onward transfer situations. This assessment must be carried out in order to determine whether the safeguards established by the BCRs can be respected in practice, taking into account the circumstances of the transfer and the conflicts that may exist between the requirements of the law of the third country and fundamental rights. If this is not the case, the data exporter located in a Member State, where appropriate in collaboration with the data importer, must assess whether it can provide for additional measures to ensure a substantially equivalent level of protection. to that guaranteed within the EEA. The implementation of the additional measures is the responsibility of the exporter, including after the approval of the BCRs by the competent authority. Consequently, these additional measures are not part of the elements analyzed within the

framework of the BCR approval procedure. In the event that the data exporter established in a Member State is not able to take additional measures sufficient to ensure a level of protection substantially equivalent to that guaranteed in the Union, there can be no transfer of personal data to the third country under the BCRs. Therefore, the data exporter is obliged to waive, suspend or terminate the transfer of personal data. In the same logic, when the exporter becomes aware of new developments affecting data protection in a third country which reduce the level of protection expected; he is required to suspend or terminate the transfer concerned. In accordance with the cooperation procedure described in working document WP263.rev.01, the documentation relating to the Leyton group's subcontractor BCRs has been examined by the CNIL services as competent authority, then by the services of two other data protection authorities acting as co-instructors. These BCRs have also been reviewed by the data protection authorities of the member countries of the EEA pursuant to the approval procedure set up by the European Data Protection Board (EDPS). The instruction of the BCRs under -contractor of the Leyton group makes it possible to conclude that these comply with the requirements imposed by article 47-1 of the GDPR and the working document WP257.rev.01, in particular because the aforementioned BCRs: i. are made legally binding by an intra-group contract and impose a clear obligation on each participating entity of the Leyton Group, including their employees, to comply with them (Articles 4.1, 6.1.1 and 6.1.2 of the BCRs); ii. expressly confer rights on the persons concerned allowing them to avail themselves of them as third-party beneficiaries via article 8.2 of the BCRs; iii. meet the requirements imposed by Article 47-2 of the GDPR: the structure and contact details of the group of companies and each of its entities are detailed in the WP265 form which was provided as part of the examination of the file and in Annex 1 of the BCRs; the transfers or all transfers of data, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the name of the country or countries third parties in question are specified in article 5 and in appendix 1 of the BCRs; the legally binding nature, both internal and external, of the subcontractor BCRs is recognized in article 6.1 of the BCRs as well as in article 5 the draft intra-group contract provided by the group; the application of general principles relating to data protection, in particular limitation of purpose, minimization of data, limitation of data retention periods, data quality , data protection by design and data protection by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, as well as data protection requirements. subsequent transfers to organizations that are not bound by the Binding Corporate Rules are referred to in Articles 5.2, 5.3, 6.3, 6.6.1, 6.7 and 6.8 of the BCRs and in Annexes 2 and 3 of the BCRs; the right to introduce a claim with the competent supervisory authority and before the competent courts of the Member

States in accordance with Article 79 of the GDPR and to obtain redress and, where applicable, compensation for breach of the binding corporate rules, are provided for in Articles 7 and 8 of the BCRs; the acceptance, by the processor established on the territory of a Member State, of the engagement of its responsibility for any violation of the binding corporate rules by any entity concerned not established in the Union is clarified in Article 7 of the BCRs, as is the principle according to which the exemption, in whole or in part, from this liability can occur only if the interested party proves that the event giving rise to the damage is not not attributable to the entity in question; the way in which information on the binding corporate rules, in particular with regard to the elements mentioned in points d), e) and f) of Article 47.2 of the GDPR are provided to data subjects, in addition to the information referred to in Articles 13 and 14 of the GDPR is specified in Article 9 of the BCRs; the missions of any data protection officer, appointed in accordance with Article 37, or of any other person or entity responsible for monitoring compliance with the binding corporate rules within the group of companies, or the group of companies engaged in a joint economic activity, as well as the monitoring of training and the handling of complaints, are detailed in Article 10 of the BCRs; Complaints procedures including the obligation of Leyton as processor to inform the controller of the complaint or request, are described in Articles 6.2, 6.6.1 and 8 of the BCRs; the mechanisms put in place within the group of companies to ensure monitoring of compliance with the binding corporate rules are detailed in Article 12 of the BCRs. These mechanisms include data protection audits and methods to ensure that corrective action will be taken to protect the rights of the data subject. The results of these checks are communicated to the person or entity referred to in point h) above and to the board of directors of the undertaking which exercises control over the group of undertakings (in this case, at the head office Leyton's corporate and privacy team), and are available to the relevant supervisory authority upon request; the mechanisms in place to communicate and log changes to the rules and to communicate these changes to the supervisory authority are specified in Article 11 of the BCRs; the cooperation mechanism with the supervisory authority put in place to ensure compliance with the rules by all entities of the group of companies is described in Article 13 of the BCRs. The obligation to make available to the supervisory authority the results of the checks of the measures referred to in point j) above is specified by this same article; the mechanisms for communicating to the competent supervisory authority all the legal obligations to which a corporate group entity is subject in a third country which are likely to have a material adverse effect on the safeguards provided by the binding corporate rules are described in Article 16 of the BCRs; finally, Article 6.1.2.3 of the BCRs provide for appropriate data protection training for staff with permanent or regular access to personal data. in article 64-1-f of the GDPR. The Commission has taken this opinion into

account. Decides: The CNIL approves the subcontractor BCRs presented by the Leyton group, insofar as they provide appropriate guarantees for the transfer of personal data in accordance with Articles 46-1, 46 -2-b, 47-1 and 47-2 of the GDPR. In order to dispel any ambiguity, the CNIL recalls that the approval of the BCRs does not imply the approval of specific transfers of personal data carried out on the basis of the BCRs. Consequently, the approval of the BCRs cannot be interpreted as the approval of transfers to third countries included in the BCRs for which a level of protection substantially equivalent to that ensured within the EU cannot be guaranteed. implementation of the approved BCRs does not require specific additional authorization from the European data protection authorities concerned. In accordance with Article 58-2-j of the GDPR, each data protection authority concerned has the power to order the suspension of data flows sent to a recipient located in a third country or to an international organization in the event that the appropriate guarantees provided for by the Leyton group's subcontractor BCRs are not respected. The President Marie-Laure DENIS This decision may be the subject of an appeal before the Council of State within two months of its notification.APPENDIX TO THE DRAFT DECISION next application:A. Scope. These Processor BCRs apply where Leyton is acting as a processor on behalf of and under the instructions of a controller established in the EU who is not a Leyton group entity (Article 1 of the BCRs).B. EEA member states from which the transfers are made: France, Italy, Germany, Spain, Poland, Portugal, Belgium, the Netherlands and Sweden (annex 1 of the BCRs).C. Third countries to which transfers are made: transfers of personal data are made to entities of the Leyton group located in Morocco, Canada and the United Kingdom (appendix 1 of the BCRs).D. The purposes of the transfers: the purposes are detailed in article 5.2 of the BCRs. They depend on the services provided to the controller and correspond to the following activities: support in terms of savings or financing levers generated in particular by:
tax incentive schemes for research and innovation, the Research Tax Credit (CIR) and aid and subsidies; the delivery of Energy Savings Certificates (CEE) or other national white certificate scheme; optimization of local and national taxation; optimization of corporate taxation; optimization of energy taxation; optimization of social charges; optimization of rental charges; optimization of the allocation of resources of the company (telecommunications, car fleet, temporary work, energy expenses, insurance, etc.) the recovery of daily allowances from Customers' employees (IJSS), the payment of the Transport Payment (VT) contribution to which Customers are subject, the management of medical visits (VM), training and declarations of accidents at work (AT); the supply and maintenance of software; the analysis and control of the processing of invoices and the collection of cash.E. Categories of data subjects: these categories are listed in article 5.4 of the BCRs as follows:

Customers' personnel (employees, temporary workers, trainees, etc.); Customers' contractual partners or their representatives and their potential Customers, as where appropriate; third parties likely to intervene in the context of the Services (in particular court officers, representatives appointed by a court, etc.). F. Categories of personal data transferred: these categories are listed by article 5.3 of the BCR as follows: identification information (first name, surname, date and place of birth; social security number); data relating to life private (address, contact details, number of children, marital status, etc.); data relating to professional life (job title, curriculum vitae, employee number, information relating to pay, information relating to training, etc.)); data relating to economic and financial life (tax identification number, etc.); data relating to health (information relating to an accident at work and sick leave, etc.).