

Paris, June 23 2022

## THE CHAIRMAN

Mister Commissioner,

The free movement of data, like the free movement of people, capital, goods and services, is an essential element of the future prosperity of the European Union. In order to develop, this freedom requires a trustworthy framework to ensure the security of sensitive business and public administration data in the cloud. However, the current situation is not conducive to the development of this freedom of data flow. Many organisations, both public and private, are obliged to maintain data hosting, and associated processing, on their premises because of the sensitivity of the data to illegal international access by non-European administrative and judicial authorities through legislation with extraterritorial reach.

The European Union has to face in all its dimensions the consequences of the judgment of the Court of Justice of the European Union of 16 July 2020 in the so-called "Schrems II" case, which invalidated the Privacy Shield adequacy agreement. The situation highlighted by the Court of Justice of the European Union for personal data is also relevant for sensitive non-personal data of European public and private organisations. The cloud, with its exponential growth in the European market, and the hegemonic capture of this market by hyperscalers, offers non-European state authorities a means, unparalleled in history, of gaining massive access to the sensitive data of the European economy. Faced with this threat, the European Union must equip itself with mechanisms that are equal to this threat and that allow it to guarantee the free circulation of sensitive data of European public and private organisations under conditions of verifiable and opposable trust.

In this context, we welcome the draft Data Regulation which aims at implementing horizontally applicable safeguards to strengthen the protection of non-personal data hosted in Europe from international access. In addition to these ambitious provisions, we call for a European Certification Scheme for Cloud Services (EUCS) to ensure the highest level of immunity to non-European legislation with extraterritorial reach for certain cloud service offerings on the European market. We believe that the implementation of an ambitious certification scheme follows from the spirit of the Cybersecurity Act, whose objective is to establish a harmonised regulatory framework guaranteeing the protection and security of information systems and data within the European Union.

Our continent, after having been at the forefront of personal data protection, a fundamental right that is now recognised, must, in our opinion, equip itself with the instruments to protect the sensitive non-personal data of its industries and services. Large companies and public administrations, all users of cloud

services, therefore expect the European Union to address this challenge by incorporating criteria for immunity to non-European legislation with extraterritorial reach into the highest level of the next European certification scheme. This highest level is an essential element of the trust framework that European organisations, both public and private, most need to protect their sensitive data, and to which the European cloud services market is currently unable to provide an adequate response. Apart from this specific need, we are convinced that the bulk of European users' use cases will necessarily be covered by the basic and substantial levels of the European cloud services certification scheme.

Furthermore, we would like to draw your attention to the labelling of services developed within the framework of the AISBL Gaia-X, which brings together European and non-European organisations and which meets a need expressed at European level by both cloud service providers and their users. Level 3 of the Gaia-X labels explicitly provides for immunity from non-European legislation with extraterritorial scope. The legal analyses carried out by AISBL Gaia-X in the context of the work on the labels have shown that a high level guaranteeing immunity to non-European legislation does not present a risk with regard to competition law and international treaties, provided that there are alternatives with the basic and substantial levels.

If the European Union were to give up defining a high level of certification, guaranteeing immunity to non-European legislation with extraterritorial scope, if it were naive enough to give in to pressure from its geopolitical competitors who do not have the same modesty when it comes to protecting their sensitive data in the cloud, it would deprive European organisations, both public and private, of the full economic and technological benefits brought about by the use of the cloud, which is now so essential to our economy.

Under these conditions, Commissioner, we call on the European Commission to firmly arbitrate in favour of a high level of security in the third level of the future certification scheme for European Union cloud services, making it possible to guarantee the immunity of the sensitive data of European public and private organisations with regard to extra-European legislation with an extraterritorial scope, in line with the need expressed by European players, suppliers and users, in the context of Gaia-X.

Yours sincerely,

Jean-Claude Laroche,

Chairman of Cigref