FRENCH REPUBLIC

The Prime Minister

Draft Decree on the protection of strategic and sensitive data in the cloud computing market

NOR:

Target audience: *State administrations and operators, public interest groups*

Subject: *…*

Entry into force: *the Decree shall enter into force on the day after its publication.*

Notice: *….*

References: *The Decree implements Article 31 of Law No 2024-449 of 21 May 2024 on securing and regulating the digital space. It may be consulted on the Légifrance website (http://www.legifrance.gouv.fr).*

The Prime Minister,

On the report of XX,

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No 526/2013;

Having regard to Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services;

Having regard to the Defence Code, particularly Article D. 3126-2;

Having regard to Order No 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities, in particular Article 9 thereof;

Having regard to Law No 2016-1321 of 7 October 2016 for a Digital Republic, in particular Article 16 thereof;

Having regard to Law No 2024-449 of 21 May 2024 on securing and regulating the digital space, in particular Article 31 thereof;

Having regard to Decree No 2014-445 of 30 April 2014 on the tasks and organisation of the Directorate-General for Internal Security;

Having regard to Decree No 2015-350 of 27 March 2015, as amended, on the qualification of security products and trust service providers for the security needs of information systems;

Having regard to notification No XX sent to the European Commission on XXX;

Having consulted the Council of State (Administration Section),

Decrees:

Article 1

The list of public interest groups referred to in Article 31(I) of the aforementioned Law of 21 May 2024 includes:

- The public interest group known as the 'Digital Health Agency (ANS)';
- The public interest group known as the 'National Agency for AIDS Research (ANRS)';
- The public interest group known as the 'Agency for the Promotion of Educational and Scientific Training and Exchange';
- The public interest group 'Secure Data Access Centre (CASD)';
- The public interest group 'Resource Centre for the Prevention of Radicalisation';
- The public interest group 'National Veterinary School';
- The public interest group 'Public Interest Group on High Activity Sealed Radioactive Sources (GIP SOURCES HA)';
- The public interest group 'National System for Registering Demand for Social Housing (GIP SNE)';
- The public interest group 'Modernisation of Social Declarations (GIP-MDS)';
- The public interest group 'Science and Technology Observatory'.

Article 2

I - For the application of Article 31 of the aforementioned Law of 21 May 2024, the private service provider must implement the following security and data protection criteria:

- a documented information security and risk management policy incorporating the subcontracting chain;
- a secure human resources management system for staff involved in the provision of the service;

- tools and procedures for the secure management of equipment implementing the service and information systems;
- physical, environmental, and logical security measures, such as the use of encryption mechanisms, access control, and user identity management;
- information security incident management procedures and business continuity measures;
- measures for compliance with the legal provisions in force in France and data protection measures, in particular contractual ones, for processed or stored data against any access by public authorities of third countries not authorised by European Union law or the law of a Member State, including in particular conditions governing the holding of capital and voting rights in the service provider's company and the establishment of the service provider and any subcontractors.

A framework, developed by the French Cybersecurity Agency under the conditions of the aforementioned Decree of 27 March 2015, lays down the requirements relating to those criteria. The consultation necessary for the creation and development of this reference framework for the State information system shall be conducted in conjunction with the Interministerial Digital Directorate.

II - In order to meet the data protection and security requirements laid down in Article 31(I) of the aforementioned Law of 21 May 2024, the administrations concerned shall have recourse to cloud computing services provided by a qualified private service provider, awarded under the conditions laid down in Chapter III of the aforementioned Decree of 27 March 2015 and meeting the criteria referred to in point I of this Article, or of a European certification of at least an equivalent level.

III - Operational and communication information systems, scientific and technical information systems, and information systems that involve, require, or contain classified media or information comprising the defence information and communication system, as well as the information and communication systems operated by the services referred to in Article D. 3126-2 of the Defence Code and Article 1 of the above-mentioned Decree of 30 April 2014, are excluded from the scope of this Article.

Article 3

I - Where an administration has already initiated, on the date of entry into force of Article 31 of the aforementioned Law of 21 May 2024, a project fulfilling the conditions laid down in the aforementioned Article and using a cloud computing service provided by a private service provider not implementing the security and data protection criteria defined in Article 2 of this Decree, it may request, in accordance with the procedures laid down by order of the Prime Minister, a derogation from the obligations laid down in the same Article.

This derogation may not exceed 18 months where there is an acceptable offer of cloud computing services, within the meaning of point II of this Article, available in France. Where there is no acceptable cloud offer available in France at the date of the request for derogation, the derogation may not exceed one year before a possible new request.

This derogation is granted by a reasoned decision of the Minister responsible for the project and validated by the Prime Minister.

It shall be made public under the conditions laid down in Book III of the Public Relations Code.

II – The assessment of the acceptability, within the meaning of Article 31(III) of the Law of 21 May 2024 referred to above, of a cloud computing services offer is based on the following criteria:

- the functional need which the offer is able to meet, taking into account the tasks of the administration concerned;
- the financial conditions;
- the operational and technical conditions of data security and protection for the data processed by the provider of the offer in accordance with the requirements laid down in Article 2 of this Decree;
- the end-of-contract conditions and reversibility guarantees;
- the control, sustainability and independence conditions within the meaning of Article 16 of the aforementioned Law of 7 October 2016.

Done on,

By the Prime Minister: