EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

France

Decree No. 2018-384 of 23 May 2018 on the security of the networks and information systems of critical service operators and digital service providers

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: France

Decree No. 2018-384 of 23 May 2018 on the security of the networks and information systems of critical service operators and digital service providers

JORF no. 0118 of 25 May 2018

The Prime Minister,
Having regard to the Commission's implementing regulations (EU) 2018/151 of 30 January laying down detailed rules for the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council specifying the elements to be taken into account by digital service providers in managing risks that threaten the security of networks and information systems and the parameters for determining whether an incident has a significant impact;
Having regard to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of security of networks and information systems in the Union;
Having regard to the Defence Code, in particular Articles L. 2321-1, R.* 1132-3 and R. 2321-1;
Having regard to Act No. 2018-133 of 26 February 2018 containing various provisions for adapting to European Union law in the field of security, in particular Title I thereof;
Having regard to Decree No. 97-1184 of 19 December 1997, as amended, adopted for the application to the Prime Minister of 1° of Article 2 of Decree No. 97-34 of 15 January 1997 on the decentralisation of individual administrative decisions;
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 purposes of national security;
The Council of State (Administration Section) having been heard,
Decrees:

Chapter I: Provisions on the security of networks and information systems of operators of critical services (Articles 1 to 15)

Section 1: Designation of essential service operators (Articles 1 to 6)

Article 1

The list of services essential to the functioning of society or the economy mentioned in Article 5 of the aforementioned Act of 26 February 2018 is set out in the Appendix to this Decree.

Article 2

Operators providing at least one service mentioned in the Annex to this Decree are designated as critical service operators, pursuant to Article 5 of the aforementioned Act of 26 February 2018, when networks and information systems are necessary for the provision of this service and an incident affecting such networks and systems would have serious consequences on its provision, assessed with regard to the following criteria:

1. The number of users depending on the service;

2. the dependence of the other sectors of activity listed in the appendix to this Order on the service;

3. The consequences of any incident, in terms of severity and duration, on the functioning of the economy or society or on public security;

4. The operator's market share;

5. The geographical scope in terms of the area likely to be affected by an incident;

6. The importance of the operator in ensuring an adequate level of service, taking into account the availability of alternative means of providing the service;

7. As applicable, sectoral factors.

Article 3

Operators of critical services are designated by order of the Prime Minister. This decree mentions the services essential to the functioning of society or the economy provided by the operator. The Prime Minister shall notify each operator concerned of his intention to designate it as an operator of critical services. The operator shall have a period of one month from the date of notification to submit any observations. Where the operator whose designation is envisaged provides a critical service in one or more other EU Member States, its designation shall be preceded by prior consultation of the Member States concerned. The orders referred to in the first subparagraph shall be notified to the operators concerned.

Article 4

For the designation of critical service operators, each minister whose remit covers a sector or sub-sector of activities listed in the appendix to this decree shall propose a list of operators to the Prime Minister, falling within this sector or sub-sector, likely to be designated as critical service operators, justifying, for each operator, their proposal with regard to the criteria mentioned in Article 2. The National Agency for Information Systems Security may also, after consulting the ministers concerned, propose to the Prime Minister, under the same conditions, the designation of operators of critical services for all sectors and sub-sectors of activity listed in the appendix to this decree.

Article 5

Each critical service operator shall appoint a person to represent it before the National Agency for Information Systems Security for all matters relating to the application of the provisions of this chapter. It shall provide this agency with the details of this person within two months of the date on which the order mentioned in Article 3 takes effect.

Article 6

The Prime Minister, on the proposal of the minister whose remit covers a sector or sub-sector of activities listed in the appendix to this decree or of the National Agency for the Security of Information Systems, shall terminate the designation of critical service operators who no longer meet the criteria mentioned in Article 2.

Section 2: Declaration of networks and information systems (Articles 7 to 9)

Article 7

Operators of critical services shall draw up and keep up to date the list of networks and information systems mentioned in the first paragraph of Article 5 of the aforementioned Act of 26 February 2018, to which the security rules provided for in Article 6 of the same Act apply. This list shall include, as applicable, networks and information systems whose operation they have entrusted to a third party where such networks and information systems are necessary for the provision of the operator's critical services.

Article 8

Within three months of its designation as an operator of critical services, the operator shall provide the National Agency for Information Systems Security, in accordance with the procedures set by order of the Prime Minister, with the list mentioned in Article 7 and, for each network and information system, the information specified by this order.

Once a year, the operator shall provide the National Agency for Information Systems Security with updates to the list and the information mentioned in the first paragraph. It shall keep this list and this information available to the Agency, in particular with a view to the checks provided for in Section 5 of this Chapter. It shall evidence any removal of networks and information systems previously included in this list.

Article 9

The National Agency for Information Systems Security may, after receiving the opinion of the ministers concerned, make comments to the operator of critical services on the list mentioned in Article 7 and the information mentioned in Article 8. In this case, the operator amends its list and the information in accordance with these observations and shall pass the amended list and information on to the Agency within two months of receipt of the observations.

Section 3: Security rules (Article 10)

Article 10

A Prime Ministerial order shall set, at the proposal of the National Agency for the Security of Information Systems, the security rules provided for in Article 6 of the aforementioned Act of 26 February 2018 and the time limits within which they shall apply. These rules bear:

1. In the field of network and information system security governance, on the development and implementation of a network and information system security policy and network and information system security certification;

2. In the field of network and information system protection, on the security of the architecture and administration of networks and information systems and access controls to these networks and systems;

3. In the field of network and information system defence, on the detection and handling of security incidents affecting networks and information systems;

4. In the field of business resilience, on crisis management in the event of security incidents having a major impact on critical services.

Section 4: Reporting of security incidents (Articles 11 to 12)

Article 11

Without prejudice to sectoral provisions providing for other incident reporting systems, operators of critical services shall report to the National Agency for Information Systems Security, as soon as they become aware of them, the incidents mentioned in I of Article 7 of the aforementioned Act of 26 February 2018.

As soon as they become aware of additional information relating to the causes of the incident or its consequences, including, as applicable, information on the provision of the service in other Member States of the European Union, operators shall pass this information on to the Agency. They must also respond to the agency's requests for information about the incident as it develops. A Prime Ministerial order sets out the procedures for reporting incidents.

Article 12

After each incident mentioned in I of Article 7 of the aforementioned Act of 26 February 2018, the National Agency for the Security of Information Systems shall send a summary of the information gathered to the relevant ministers.

It shall inform the competent authorities or bodies of other EU Member States of the incidents mentioned in the first subparagraph which have a significant impact on the continuity of critical services provided in those States. Under the conditions provided for by II of the same Article 7, it may, at the request of the Prime Minister, inform the public of the incidents mentioned in the first paragraph that have been reported to it.

Section 5: Security checks (Articles 13 to 15)

Article 13

The Prime Minister, after receiving the opinion of the relevant ministers, shall notify operators of critical services of his decision to impose checks provided for in Article 8 of the aforementioned Act of 26 February 2018. He shall specify the objectives and scope of the audit and set the deadline by which the audit must be carried out. He shall indicate, depending on the nature of the operations to be carried out, whether this check is carried out by the National Agency for the security of information systems or by a qualified service provider. In the latter case, the operator shall choose the provider from the list supplied to him and shall inform the National Agency for the Security of Information Systems of this without delay.

The Prime Minister may not impose more than one inspection per calendar year of the same network and information system on an operator, unless the operator's network and information system is affected by a security incident or if vulnerabilities in this network and information system or breaches of the security rules mentioned in Article 6 of the aforementioned Act of 26 February 2018 have been observed during a previous inspection undergone by the operator.

Article 14

To perform the check, the operator of critical services shall conclude an agreement with the National Agency for the Security of Information Systems or the provider responsible for carrying out the checks. This agreement shall specify:

1. The objectives and scope of the audit ;

2. The procedures for the conduct of the inspection and the deadline by which it is to be completed;

3. The conditions under which the agency or the provider access networks and information systems and carry out analyses and readings of technical information;

4. The information and elements, particularly the technical documentation of the hardware and software, that the operator passes on to the agency or the service provider for the performance of the check; 5. The conditions for protecting the confidentiality of the information processed in the framework of the check.

The agreement shall be concluded within a time frame consistent with the deadline set by the Prime Minister for the completion of the inspection. Where the check is carried out by a provider, the operator shall send a copy of the signed agreement to the Agency without delay.

Article 15

At the end of the inspection, the National Agency for the Security of Information Systems or the provider that carried out the inspection shall draw up a report setting out its findings, with regard to the purpose of the inspection, on compliance with the obligations set out in Chapter II of Title I of the aforementioned Act of 26 February 2018 and on the level of security of the networks and information systems inspected. Any breaches of these obligations and vulnerabilities in networks and information systems found during the audit shall be indicated in the report, which shall make recommendations for remedying them as applicable. The agency or service provider that carried out the check shall give the critical service operator the opportunity of commenting on the report referred to in the first paragraph.

Where the inspection is carried out by a provider, it shall send the report referred to in the first subparagraph and, as applicable, the operator's comments, to the Agency, within the time limit set for carrying out the inspection. The Agency may, within two months of receiving the report, interview the provider that carried out the inspection, in the presence of the operator, if the latter has made observations or if the Agency so requests, and of a representative of the relevant ministers, if they so wish, to examine the findings and recommendations contained in the report. The National Agency for the Security of Information Systems shall convey the conclusions of the audit to the ministers concerned.

Chapter II: Provisions on the security of networks and information systems of digital service providers (Articles 16 to 24)

Section 1: Designation of representatives of digital service providers (Article 16)

Article 16

Digital service providers who, pursuant to I of Article 11 of the aforementioned Act of 26 February 2018, designate a representative on domestic soil, shall inform the National Agency for the Security of Information Systems thereof by providing it, within two months of such designation, with the contact details of their representative. The Agency shall inform the relevant ministers of this. The representative referred to in the first paragraph shall act on behalf of the digital service provider to meet the obligations set out in this chapter. In particular, he shall represent the provider before the Agency in all matters relating to the application of the provisions of this Chapter.

Section 2: List of networks and information systems (Article 17)

Article 17

Digital service providers shall draw up and keep up to date the list of networks and information systems mentioned in Article 12 of the aforementioned Act of 26 February 2018, to which the measures provided for in the same Article shall apply. This list shall include, as applicable, networks and information systems whose operation they have entrusted to a third party where such networks and information systems are necessary for the provision of digital services.

Section 3: Security measures (Articles 18 to 19)

Article 18

The nature of the measures that digital service providers are required to implement in accordance with Article 12 of the aforementioned Act of 26 February 2018 is set out in Article 2 of the aforementioned implementing regulation of 30 January 2018.

Article 19

Digital service providers shall provide the National Agency for the Security of Information Systems, with a view to the checks provided for in Section 5 of this chapter, with the list of networks and information systems mentioned in Article 17 as well as the documents making it possible to verify the implementation of the measures mentioned in Article 12 of the aforementioned Act of 26 February 2018.

Section 4: Reporting of security incidents (Articles 20 to 21)

Article 20

Without prejudice to sectoral provisions providing for other incident reporting regimes, digital service providers shall report any incident with a significant impact on the provision of their services to the National Agency for Information Systems Security, pursuant to I of Article 13 of the aforementioned Act of 26 February 2018. In determining whether an incident has a significant impact on the provision of their services, digital service providers shall consider the parameters mentioned in Articles 3 and 4 of the aforementioned Implementing Regulation of 30 January 2018.

Digital service providers respond to the agency's requests for information about the incident as it develops. A Prime Ministerial order sets out the procedures for reporting incidents.

Article 21

After each incident mentioned in I of Article 13 of the aforementioned Act of 26 February 2018, the National Agency for the Security of Information Systems shall send a summary of the information gathered to the relevant ministers.

It shall inform the competent authorities or bodies of other EU Member States of the incidents mentioned in the first subparagraph which have a significant impact on the digital services provided in those States.

Under the conditions provided for in II of Article 13 of the aforementioned Act of 26 February 2018, the Prime Minister may ask the National Agency for the Security of Information Systems to inform the public of an incident mentioned in the first paragraph or require the relevant digital service provider to do so. In the latter case, the Prime Minister shall specify the information to be made public and the deadline for doing so. The must make this information available to the public by means of the website used for the provision of the service, unless this website is unavailable due to the incident, such that this information is presented to users when they access the service.

Section 5: Security checks (Articles 22 to 24)

Article 22

The Prime Minister shall notify the digital service providers of his decision to impose a check provided for in Article 14 of the aforementioned Act of 26 February 2018. He shall specify the objectives and scope of the audit and set the deadline by which the audit must be carried out. He shall indicate, depending on the nature of the operations to be carried out, whether this check is carried out by the National Agency for the security of information systems or by a qualified service provider. In the latter case, the digital service provider shall choose the provider from the list provided to it and shall inform the agency without delay.

Article 23

To perform the check, the provider of digital services shall conclude an agreement with the National Agency for the Security of Information Systems or the provider responsible for carrying out the checks. This agreement shall specify:

1. The objectives and scope of the audit ;

2. The procedures for the conduct of the inspection and the deadline by which it is to be completed;

3. The conditions under which the agency or the provider access networks and information systems and carry out analyses and readings of technical information;

4. The information and elements, in particular the technical documentation of the hardware and software, that the digital service provider conveys to the agency or the provider for the performance of the check;

5. The conditions for protecting the confidentiality of the information processed in the framework of the check.

The agreement shall be concluded within a time frame consistent with the deadline set by the Prime Minister for the completion of the inspection. Where the check is carried out by a provider, the provider of digital services shall send a copy of the signed agreement to the Agency without delay.

Article 24

At the end of the inspection, the National Agency for the Security of Information Systems or the provider that carried out the inspection shall draw up a report setting out its findings, with regard to the purpose of the inspection, on compliance with the obligations set out in articles 12 and 13 of Title I of the aforementioned Act of 26 February 2018 and on the level of security of the networks and information systems inspected. Any breaches of these obligations and vulnerabilities in networks and

information systems found during the audit shall be indicated in the report, which shall make recommendations for remedying them as applicable.

The agency or provider that carried out the check shall give the provider of digital services the opportunity of commenting on the report referred to in the first paragraph.

Where the inspection is carried out by a provider, it shall send the report referred to in the first subparagraph and, as applicable, the comments of the provider of digital services, to the Agency, within the time limit set for carrying out the inspection. The Agency may, within two months of receiving the report, interview the provider that carried out the inspection, in the presence of the provider of digital services, if the latter has made observations or if the Agency so requests, and of a representative of the relevant ministers, if they so wish, to examine the findings and recommendations contained in the report.

The National Agency for the Security of Information Systems shall convey the conclusions of the audit to the ministers concerned.

Chapter III: Miscellaneous and final provisions (Articles 25 to 33)

Article 25

The operators of critical services mentioned in Chapter I and the digital service providers mentioned in Chapter II shall take the necessary measures to ensure the application of the provisions laid down in this decree to the networks and information systems that are necessary for the provision of their services and whose operation they have entrusted to third parties.

Article 26

The service providers authorised to perform the checks provided for in Articles 8 and 14 of the aforementioned Act of 26 February 2018 are qualified under the conditions provided for in Chapter III of the aforementioned Decree of 27 March 2015.

Article 27

The cost of the checks carried out by the National Agency for the security of information systems pursuant to Articles 8 and 14 of the aforementioned Act of 26 February 2018 shall be calculated based on the time required to carry out the check and the number of public officials involved. The cost of a check involving a public official for one day is set by order of the Prime Minister.

The cost of checks carried out by a service provider shall be freely determined by the parties.

Article 28

Any contentious appeal filed by a critical service operator or a digital service provider against individual decisions taken regarding it on the basis of this decree shall be preceded, on pain of inadmissibility, by a prior administrative appeal to the Prime Minister.

Article 29

Modified the following provisions

Modifies Decree No. 2009-834 of 7 July 2009 - art. 4 (M)

Modifies Decree No. 2015-350 of 27 March 2015 (V)

Modifies Decree No. 2015-350 of 27 March 2015 - art. 1 (V)

Modifies Decree No. 2015-350 of 27 March 2015 - art. 10 (V)

Modifies Decree No. 2015-350 of 27 March 2015 - art. 18 (V)

Modifies Decree No. 2015-350 of 27 March 2015 - art. 25 (V)

Modifies Decree No. 2015-350 of 27 March 2015 - art. 26 (V)

Modifies Order of 10 June 2016 - art. Appendix I (V)

Modifies Order of 17 June 2016 - art. (V)

Modifies Order of 17 June 2016 - art. (V)

Modifies Order of 28 November 2016 - art. (V)

Modifies Order of 28 November 2016 - art. (V)

Modifies Order of 28 November 2016 - art. (V)

Modifies Order of 28 November 2016 - art. (V)

Modifies Order of March 10, 2017 - art. Schedule I (V)

Modifies the Defence Code. - art. R1332-41-16 (V)

Modifies the Defence Code. - art. R1332-41-7 (V)

Modifies the Internal Security Code - art. R114-2 (V)

Article 30

Modified the following provisions

Modifies Decree No. 97-1184 of 19 December 1997 - art. Annex (M)

Article 31

I. - Modified the following provisions:

- Decree No. 2009-834 of 7 July 2009 Art. 3

II. - Article 3 of the aforementioned Decree of 7 July 2009, in its word as a result of I of this article, may be modified by decree.

Article 32

I. - This decree is applicable to Wallis and Futuna, French Polynesia, New Caledonia and the French Southern and Antarctic Territories.

II. - For the application of this Decree in Wallis and Futuna, French Polynesia, New Caledonia and the French Southern and Antarctic Territories, the reference to Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down detailed rules for the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council specifying the elements to be taken into account by digital service providers in managing risks that threaten the security of networks and information systems and the parameters for determining whether an incident has a significant impact, shall be replaced by the reference to the rules applicable in mainland France pursuant to that Regulation.

Article 33

This decree shall be published in the Official Gazette of the French Republic.

APPENDIX
LIST OF SERVICES CRITICAL TO THE FUNCTIONING OF SOCIETY OR THE ECONOMY

SECTOR --- Sub-sector	TYPE OF OPERATORS	CRITICAL SERVICES
ENERGY --- Electricity	Supply companies	The sale or resale of electricity to private individuals and companies (sale of electricity to end consumers, sale of electricity to electricity suppliers, operation of an electricity exchange)
	Operators of the distribution network	Electricity distribution (control and supervision of the distribution network, management of consumer connections, control of consumer meters)
	Operators of the transmission network	Electricity transmission (control and supervision of the transmission system, balancing of supply and demand, management of interconnections)
ENERGY --- Oil	Operators of oil pipelines	Oil pipeline operations (pipeline operation and supervision)
	Operators of production and refining, processing, storage and transport facilities	Production (operation and supervision of production facilities) Refining (refinery operation and supervision) Storage (operation and supervision of storage facilities) Non-pipeline transportation (transportation planning, operation of a fleet of ships or trucks)
	Operators of platforms for the transfer of digitized logistics data	Service for transferring digitized logistics data between oil operators and between oil operators and public authorities
ENERGY	Supply companies	The sale or resale of gas to individuals and companies (sale of gas to end consumers,

--- Gas		sale of gas to gas suppliers, operation of a gas exchange)
	Operators of the distribution network	Gas distribution (control and supervision of the distribution network, management of consumer connections, control of consumer meters)
	Operators of the transmission network	Gas transmission (control and supervision of the transmission system, balancing of supply and demand, management of interconnections)
	Managers of storage facilities	Gas storage (operation and supervision of storage facilities)
	Managers of liquefied natural gas facilities	Gas liquefaction (operation and supervision of liquefaction facilities) Unloading and regasification (operation and supervision of unloading facilities, operation and supervision of regasification facilities)
	Natural gas companies	Gas supply, distribution, transportation, storage and processing
	Operators of natural gas refining and processing facilities	Refining (operation and supervision of refining facilities) Processing (operation and supervision of processing facilities)
TRANSPORT --- Air transport	Air Carriers	Passenger transport (passenger check-in and boarding, aircraft operations) Cargo transport (cargo check-in and boarding, aircraft operations)
	Managers of airports and operators of ancillary facilities located at airports	Operation of airport facilities (screening, cargo check-in and boarding, passenger and baggage handling) Aircraft refuelling and crewing

	Air Navigation Services	En-route air traffic control and regulation Aerodrome control and regulation
	Aircraft maintenance companies	Aeronautical maintenance and repair
	Operators of passenger flow management systems	Passenger flow management
TRANSPORT --- Rail transport	Infrastructure managers	Rail traffic control and management (traffic supervision and regulation, signalling, switch management, traffic planning, path management)
	Infrastructure maintenance companies	Maintenance of railway infrastructure
	Railway companies	Transport of goods and hazardous materials (rolling stock operations) Passenger transport (operation of rolling stock, passenger information and reception, management of passenger flows)
	Rolling stock maintenance companies	Maintenance of rolling stock
TRANSPORT --- Guided transport	Guided transport companies	Passenger transport (operation of guided transport equipment, passenger information and reception)
TRANSPORT --- Transport by water	Inland waterway, maritime and coastal passenger and freight companies	Passenger transport (passenger flow management) Transport of goods and hazardous goods (booking, registration of goods) Route planning

	Ship maintenance companies	Ship maintenance
	Waterborne transport infrastructure operating companies	Operation of waterborne transport infrastructure
	Managers and operators of ports or harbours	Goods service (loading, unloading, storage, guarding, container management) Reception of ships (pilotage, towing, mooring, bunkering) Information, reception, screening, boarding and disembarking of passengers Management of harbour works
	Operators of maritime traffic services	Maritime Traffic Service
	Operators of river traffic services	River traffic service
TRANSPORT --- Road transport	Road authorities (public authorities)	Road management (maintenance, signalling, infrastructure management, traffic control and monitoring)
	Road infrastructure and infrastructure management companies	Road management (maintenance, signalling, infrastructure management, traffic control and monitoring)
	Operators of smart transport systems	Centralised management of a fleet of vehicles Traffic management assistance Passenger Information Operating assistance

	Goods transport companies	Transport of goods and hazardous materials
	Public road transport companies	Passenger flow management Operation
TRANSPORT	Forwarders	Organisation of transport Chartering of carriers
LOGISTICS	Managers of logistics platforms	Logistics platform management
BANKS	Credit institutions	Deposit management Granting of credits Payment service Investment service
INFRASTRUCTURES OF FINANCIAL MARKETS	Operators of trading platforms	Operation of trading platforms for financial instruments
	Central counterparts	Central counterparty service for financial market transactions (clearing houses)
	Central depositories	Record keeping Collateral management Settlement and delivery of securities
FINANCIAL SERVICES	Financial service providers, payment institutions, electronic money establishments	Payment service Issue of special securities

	Cash transport companies	Planning and operation of cash transport Management of collection and supply requests
INSURANCE	Insurance companies, mutuals, provident institutions, reinsurers	Life insurance Non-life insurance Reinsurance
SOCIAL	Social security bodies	Calculation and payment of social security benefits (health insurance, old age, family allowances and unemployment) Management of the collection and cash flow of social security bodies
JOBS AND VOCATIONAL TRAINING	Payment operators	Calculation and payment of unemployment benefits
HEALTH --- Health care facilities (including hospitals and private clinics)	Health care providers	Service contributing to prevention, diagnosis or care activities
	Providers of emergency medical assistance	Reception and governance of calls Mobile emergency and resuscitation service
HEALTH --- Pharmaceutical products	Wholesale pharmaceutical wholesalers	Pharmaceutical distribution
SUPPLY AND DISTRIBUTION OF DRINKING WATER	Suppliers and distributors of water for human consumption	Supply of bottled water (drawing, bottling, planning, logistics, water quality control) Production of running water (operation, supervision and maintenance of collection, transport, processing and storage facilities, water quality checks)

		Water distribution (operation, supervision and maintenance of water distribution facilities, logistics, water quality checks)
PROCESSING OF NON-DRINKING WATER	Wastewater collection, disposal or treatment companies	Sewage collection Sewage treatment
	Managers of floods and stormwater	Rainwater collection and drainage
DIGITAL INFRASTRUCTURES	Internet Exchange Points (IXP)	Peering service for internet traffic exchange
	Domain Name System (DNS) Service Providers	Domain name registration and management Domain name hosting Domain name resolution service
	High-level domain name registers	Assignment of domain names and management of the top-level domain name registry Hosting of top-level zones
EDUCATION	Operators in charge of the national educational pathway, operators entrusted with the organisation of national exams	Management of school or student assignments Organisation of national examinations
CATERING	Mass catering companies for the health, children and penitentiary sectors	Management of orders Management of procurement, logistics, storage and distribution

Done on 23 May 2018.