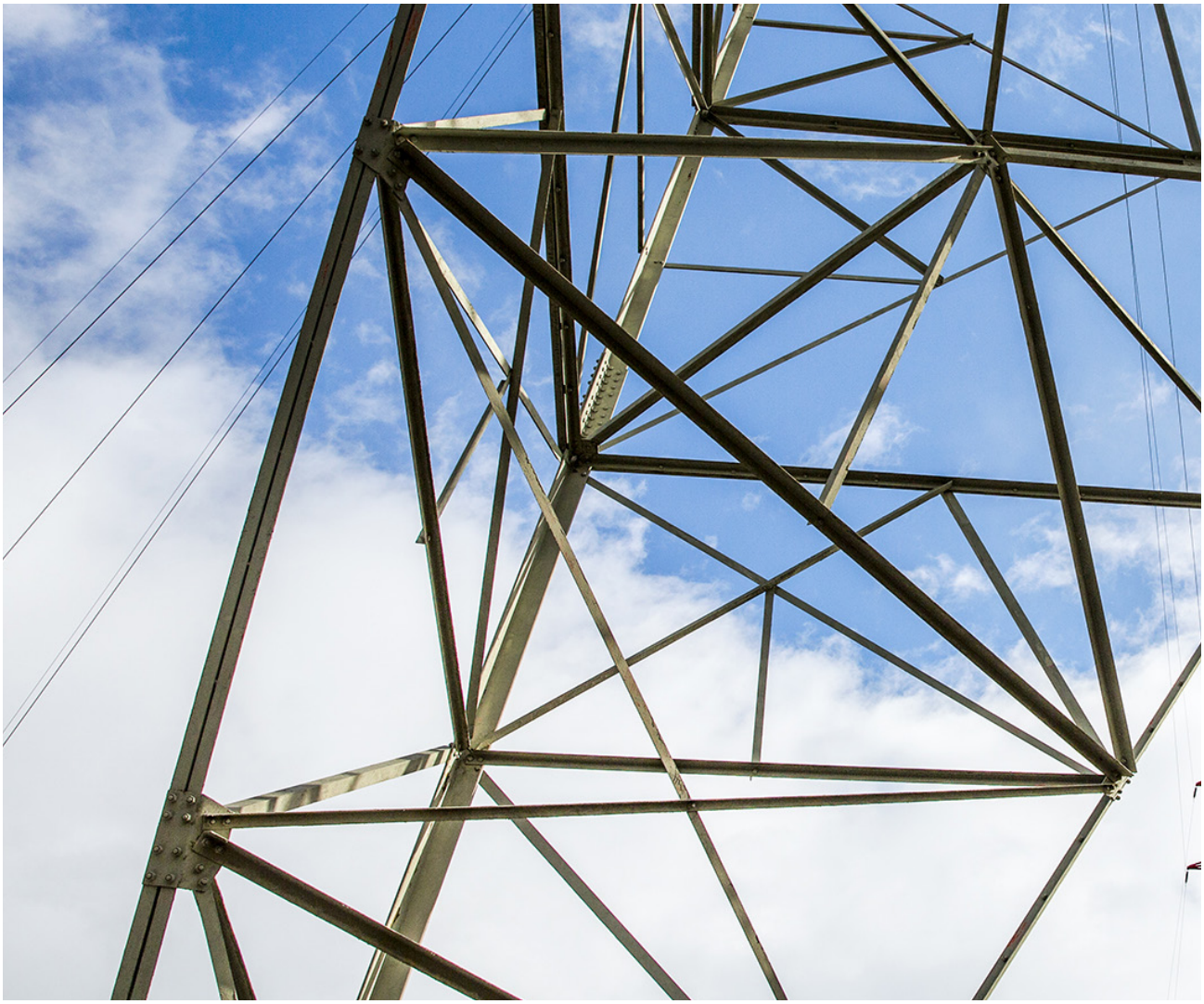
THE LEGAL AND REGULATORY LANDSCAPE FOR POWER & UTILITIES IN CENTRAL AND EASTERN EUROPE



Digital Transformation of the Power & Utilities Industry

October 2019

Microsoft

From thermal powered stations to now distributed generation using solar cells, the Power & Utilities industry has come very far. Utilities of the future are going to be self-governed and automated, leveraging digital wave which, from generation to distribution is impacting the entire value chain of this industry.

The Power & Utilities industry faces radical transformation. Distributed renewable generation, new digital technologies and AI. At the same time, changing consumer expectations are creating a new energy world that is more complex, competitive and challenging.

Fixed conventional generation is being replaced by occasional generation from renewables. Prices for new energy technologies like solar photovoltaic systems drop and enable decentralized implementations. These changes in generation patterns challenge the stability of supply to the grid and require huge investments to maintain balance and distribution reliability.

On the consumption side new innovations like electric vehicles represent other load patterns than our aging distribution grid originally was designed for. As demanding assets connected to the grid challenge distribution, connected assets can also represent a flexibility source if they are willing to change their consumption when needed. For grid operators, flexibility is key and can be an attractive alternative to costly grid investments. Private houses, commercial buildings and spaces, EVs and local small-scale production of electricity are examples of potential flexibility sources. New ways of exchanging such flexibility between a buyer and a seller are expected to arise.

Microsoft and partners leverage Azure as Cloud platform to connect flexible assets, predict and simulate bottlenecks in the grid and through artificial intelligence, enable unique insight decision support and action.

Innovative technologies collect data from the electric energy grid combined with weather forecasting, historic data analysis, and variation in energy prices to ensure a reliable and flexible availability of electric energy. All grid data is uploaded to cloud-based services enabling the electric grid to be continuously optimized with outdoor energy, increasing predictability and efficiency of the grid by predicting peak hour demand and bringing in distributed resources to reduce the demand on the substation.

Two-way flow of energy, continuous feedback loops and a changing customer role, it's a new era of the utility industry!

In order to continue towards your goals and adapt in the face of a changing industry, it will be more important than ever for you to leverage new technologies.

Microsoft helps Power & Utilities companies to become a *Digital Utility* by creating the environment for turning their multi-source data (supply-demand, distributed generation, grid, customer, prosumer, trading, weather, etc.) into business outcomes.

The legal and regulatory landscape

This Whitepaper analyses EU legislation and national legislation potentially affecting public cloud usage for the Power (electricity, coal and precious metals) and Utilities (natural gas and water supply) sectors, with emphasis on data processing, information infrastructure and information security.

The paper has been prepared with contributions from the following law firms:

- **EU SECTION & ESTONIA:** Hannes Vallikivi (Partner, Attorney-at-Law) and Margot Maksing (Associate, Attorney-at-Law), LAW FIRM DERLING PRIMUS;
- **EU SECTION & CROATIA:** Tomislav Pedišić (Attorney-at-Law) and Ivan Dušić (Attorney at Law), VUKMIR & ASSOCIATES;
- **BULGARIA:** Nikolay Zisov (Partner) and Deyan Terziev (Associate, CIPP/E), BOYANOV & CO.;
- **LATVIA:** Kristīne Gaigule – Šāvēja (Partner, Attorney-at-Law) and Kristīne Sakārne (Senior associate, Attorney-at-Law), PRIMUS DERLING, ATTORNEYS AT LAW;
- **LITHUANIA:** Tomas Venckus (Partner, Attorney-at-Law) and Greta Bagdanavičiūtė (Senior associate, Assistant Attorney-at-Law), LAW FIRM JUODKA AND PARTNERS – PRIMUS;
- **SLOVENIA:** Mateja Dren (Attorney at Law), LAW FIRM DREN & ROVŠEK SRŠE Ltd.; and
- **SERBIA:** Sanja Spasenović, (Senior Associate, independent attorney at law in cooperation with Karanovic & Partners) KARANOVIC & PARTNERS.

European Union legislation

1. Legal status of entities operating in power & utilities industry

In the EU, Cloud computing services[1] are considered digital services[2] . Multiple aspects of digital services are regulated by the Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union (generally known as the Network and Information Security directive or the **NIS Directive**).

The NIS Directive stipulates the requirements of the network and information systems of operators of essential services. Entities operating in the Power & Utilities Industry are generally considered operators of essential services. The security of energy and water supply is an essential element of public security. The criteria for the identification of the operators of essential services are:

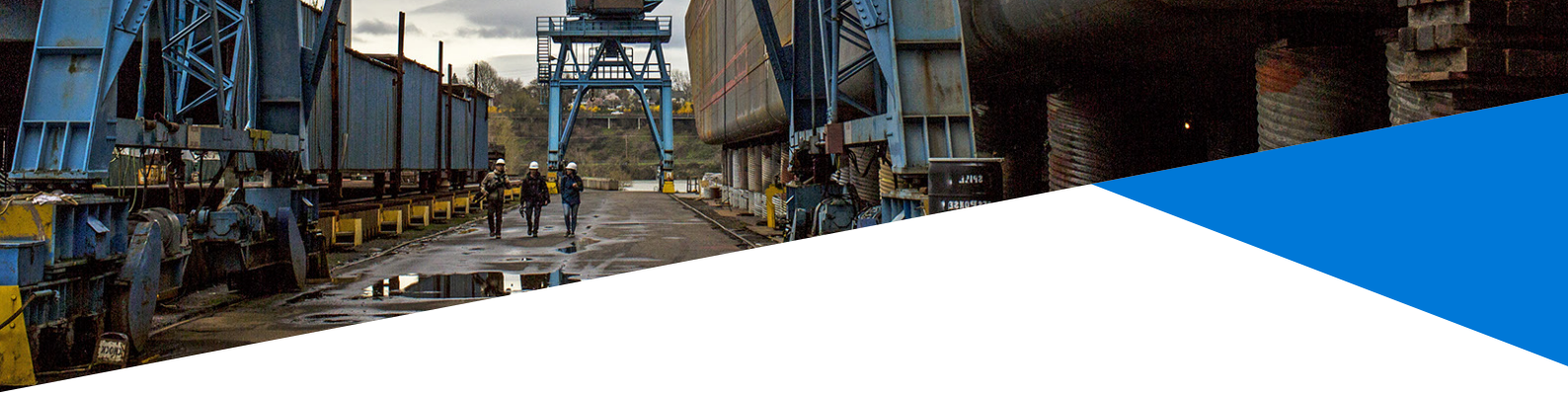
It is a public or private entity of a type referred to in Annex II of the NIS Directive (see below);

1. the entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
2. the provision of that service depends on network and information systems; and
3. an incident would have significant disruptive effects on the provision of that service.

Types of entities for the purposes of identification of the operators of essential services are stipulated in Annex II of the NIS Directive as follows:

[1] Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this Directive, the term 'cloud computing services' covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment (recital 17 of the NIS Directive).

[2] Any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. | For the purposes of this definition: | (i) | 'at a distance' means that the service is provided without the parties being simultaneously present; | (ii) | 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; | (iii) | 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. | An indicative list of services not covered by this definition is set out in Annex I (defined in Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council).



- **Electricity:** Electricity undertakings[3] which carry out the function of "supply"[4] , distribution system operators[5] and transmission system operators[6].
- **Gas:** supply undertakings[7] , distribution system operators[8] , transmission system operators[9], storage system operators[10], LNG system operators[11], natural gas undertakings[12], operators of natural gas refining and treatment facilities.
- **Drinking water supply and distribution:** Suppliers and distributors of water intended for human consumption but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services.

According to recital 19 of the NIS Directive, Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services. As a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems (recital 25 of the NIS Directive).

2. Requirements for network and information systems based on the NIS directive

There are various requirements for software solutions, information systems and digital services in general, e.g. data protection (privacy by design, privacy by default), security (Confidentiality, Integrity, Availability,Authentication, Authorization, Accountability, etc); however, we will focus solely on the requirements associated with the provision of digital services (including cloud services) to operators of essential services.

Recital 44 of the NIS Directive notes that responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. Recital 49 of NIS Directive explains that digital service providers should ensure a level of security commensurate with the degree of risk posed to the security of the digital services they provide, given the importance of their services to the operations of other businesses within the Union. In

[3] Any natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, supply, or purchase of electricity, which is responsible for the commercial, technical or maintenance tasks related to those functions, but does not include final customers (defined in Article 2(35) of Directive 2009/72/EC of the European Parliament and of the Council).

[4] The sale, including resale, of electricity to customers (defined in Article 2(19) of Directive 2009/72/EC of the European Parliament and of the Council).

[5] Natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (defined in Article of Directive 2009/72/EC of the European Parliament and of the Council).

[6] Natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (defined in Article (4) of Directive 2009/72/EC of the European Parliament and of the Council).

[7] any natural or legal person who carries out the function of supply (defined in Article 2(8) of Directive 2009/73/EC of the European Parliament and of the Council).
Natural or legal person who carries out the function of distribution and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of gas (defined in Article 2(6) of Directive 2009/73/EC of the European Parliament and of the Council).

[8] Natural or legal person who carries out the function of transmission and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transport of gas (defined in Article 2(4) of Directive 2009/73/EC of the European Parliament and of the Council).

[9] Natural or legal person who carries out the function of storage and is responsible for operating a storage facility (defined in of Article 2(10) of Directive 2009/73/EC of the European Parliament and of the Council).

[10] Natural or legal person who carries out the function of liquefaction of natural gas, or the importation, offloading, and re-gasification of LNG and is responsible for operating a LNG facility (defined in Article 2(12) of Directive 2009/73/EC of the European Parliament and of the Council).

[11] Natural or legal person carrying out at least one of the following functions: production, transmission, distribution, supply, purchase or storage of natural gas, including LNG, which is responsible for the commercial, technical and/or maintenance tasks related to those functions, but shall not include final customers (defined in Article 2(1) of Directive 2009/73/EC of the European Parliament and of the Council).

[12] All water either in its original state or after treatment, intended for drinking, cooking, food preparation or other domestic purposes, regardless of its origin and whether it is supplied from a distribution network, from a tanker, or in bottles or containers (defined in Article 2(1)(a) of Council Directive 98/83/EC).

practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is possibly higher than for digital service providers. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at Union level. Even though security requirements for operators of essential services and digital service providers may differ, if a digital service provider intends to provide services to operators of essential services, the digital services must still meet the requirements imposed on the operators of essential services.

As the NIS Directive is domestically only indirectly applicable, several of the requirements are general and require Member States to clarify the requirements within the framework of the directive.

2.1 Security of the network and information systems of digital service providers (Chapter V of NIS directive)

The security requirements are aimed at preventing risks, ensuring security of network and information systems and handling incidents. The security requirements are applicable to digital service providers regardless of whom the service is provided to.

Member States must stipulate the measures and requirements taking into account the security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing, and compliance with international standards. Member States must ensure that digital service providers notify the competent authority or the computer security incident response team (CSIRT) without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union.

Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider must be notified by that operator.

Member States may not impose any further security or notification requirements on digital service providers, unless actions are taken by Member States to safeguard their essential State functions.

The competent authorities have the necessary powers and means to require digital service providers to provide the information necessary to assess the security of their network and information systems, including documented security policies. The competent authorities can also require the digital service provider to remedy any failure to meet the requirements.

2.2 Security of the network and information systems of operators of essential services (Chapter IV of NIS directive)

The security requirements apply to the operators of essential services. However, if a digital service is provided to the operator of essential services, these requirements must be met by digital service provider as well.

Member States must ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Those measures must ensure a level of security appropriate to the risk posed. Furthermore

the operators must prevent and minimise the impact of incidents, ensure the continuity of the essential services and in case of incidents having a significant impact on the continuity, notify, without undue delay, the competent authority or the CSIRT.

2.3 The right to impose additional requirements and stricter requirements

Recital 6 of NIS Directive explains that operators of essential services and digital service providers are not precluded from implementing security measures that are stricter than those provided for under NIS Directive. Therefore, the essential service providers may require additional efforts in security. It is also noted in the recital 54 of NIS Directive that public administrations in Member States which use services offered by digital service providers, in particular cloud computing services, might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of the NIS Directive. They should be able to do so by means of contractual obligations.

According to recital 8 and Article 1(6) of the NIS Directive, the NIS Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of the essential interests of its security, to safeguard public policy and public security. It may also result in additional requirements and restrictions.

Recital 9 of the NIS Directive points out that certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive. It is therefore important to periodically review requirements at both European Union and national level.

3.EU single digital market and free flow of data

GDPR, which entered into force on May 25, 2018, confirmed free flow of personal data within the EU (see in particular sections 3, 6, 53 and 101 of the recitals, and Article 44 and 51 of the GDPR, as well as Section 1 – Context of the Proposal and section 10 of the recitals in the Proposal Regulation). Together with that legal framework concerning personal data, the current EU administration aims to put in place a comprehensive and coherent EU framework enabling free movement of all data (both personal and non-personal data) in the single market. To that effect, Regulation on Free-Flow of Non-personal Data has been enacted.

In the proposal of Regulation on Free-Flow of Non-personal Data, the European Commission holds that new digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT) are designed to maximize efficiency, enable economies of scale and develop new services. They offer benefits to users, such as agility, productivity, speed of deployment and autonomy. As indicated in the 2017 Communication "Building a European Data Economy", the value of the EU data market was estimated in 2016 at almost EUR 60 billion, showing a growth of 9.5% compared to 2015. According to a study, the EU data market could potentially amount to more than EUR 106 billion in 2020. To unlock this potential, with the Proposal Regulation, European

Commission aims to address the following issues:

- Improving the mobility of non-personal data across borders in the single market, which is limited today in many Member States by localization restrictions or legal uncertainty in the market;
- Ensuring that the powers of competent authorities to request and receive access to data for regulatory control purposes, such as for inspection and audit, remain unaffected; and
- Making it easier for professional users of data storage or other processing services to switch service providers and to port data, while not creating an excessive burden on service providers or distorting the market.

Under Article 4 of the Regulation on Free-Flow of Non-personal Data, data localization requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality. Moreover, in line with the same Article, by 30 May 2021, the Member States need to ensure that any existing data localization requirement that is laid down in a law, regulation or administrative provision of a general nature and that is not in compliance with paragraph 1 of the same Article is repealed. By 30 May 2021, if a Member State considers that an existing measure containing a data localization requirement is in compliance with paragraph 1 of Article 4 of the Regulation on Free-Flow of Non-personal Data and can therefore remain in force, it shall communicate that measure to the Commission, together with a justification for maintaining it in force.

In line with point (19) of the recitals of the Regulation on Free-Flow of Non-personal Data, the concept of 'public security', within the meaning of Article 52 Treaty on the Functioning of the European Union and as interpreted by the European Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the principle of proportionality, data localization requirements that are justified on grounds of public security should be suitable for attaining the objective pursued and should not go beyond what is necessary to attain that objective.

Therefore, in our opinion, the storage of information managed locally in the electric, natural gas, coal and precious metals, as well as water supply sectors should not be restricted to the boundaries of a Member State. The data should circulate freely within the European Union, as long as this circulation takes place in a secure environment, through reliable servers and through competent proxies. The restriction of the possibility of storing data only within the borders of a Member State should operate only in exceptional cases, based on strong justifications regarding the public security.

4. Other potentially relevant legislation

4.1 Legislation specifically applicable to power & utilities sector

As pointed out above, Power & Utilities sectors are already more regulated than other industries. A large part of the regulation concerns technical aspects of the relevant services as well as consumer protection (in terms of price and availability). In our opinion, these regulations have low relevance in relation to the use of cloud services.

Bulgaria

1. Bulgarian legislation on cloud services for critical infrastructure in the electricity, coal, precious metals, natural gas and water supply sectors

Bulgarian legislation contains limited rules and definitions expressly referring to cloud services. The Cybersecurity Act[14] defines "cloud computing service" as any digital service that enables access to a scalable and elastic pool of shareable computing resources. It imposes network and information security obligations to digital service providers, including providers of cloud computing services.

The Electronic Government Act enables the Electronic Government State Agency to build, develop and maintain shared resources of electronic government, which may include a State hybrid private cloud. The "State hybrid private cloud" is defined as a centralized state-owned information infrastructure (servers, data storage facilities, communication equipment, ancillary equipment and system software) distributed in several locations in premises complying with the criteria for building protected information centers, which provides physical and virtual resources for use and administration by State bodies, while guaranteeing a high level of security, reliability, isolation of the individual users and impossibility of interference in the operation of their information systems or unauthorized access to their information resources. The isolation of the resources and networks of the individual sector users is to be guaranteed through measures for separation on physical and logical level.

As of the date of this document, a public procurement procedure for the development, construction and commissioning of a State hybrid private cloud and a secure internet node for public e-government services is still pending, as initiated by the Electronic Government State Agency.

[14] implementing the rules of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the so-called NIS Directive)

2. Legislation regarding the energy **sector** (electricity and natural gas)

The Bulgarian Energy Act[15] and Ordinance 3 / 21.03.2013 on licensing activities in the energy sector, is the main legislation for this sector. It prescribes that energy undertakings must carry out their activities in the interest of the public and of the individual customers, ensuring the security of supply, *including protection of the sites which constitute critical infrastructure in the energy sector,* the non-interruption and the quality of electricity, heat and natural gas, the efficient utilization of fuels and energy, the protection of the environment, the life, health and property of citizens. Further, transmission system operators, transmission system owners, and distribution system operators have a confidentiality obligation with respect to trade secrets obtained in the course of carrying out their activities that could lead to commercial advantages, and must not disclose information in a discriminatory manner.

License holders are obliged to provide at the request of the Energy and Water Regulatory Commission, the Commission for Protection of Competition, and the European Commission, extensive information regarding their activities (accounting, contractual, technical, economic, etc., and keep such documentation for 5 years).

Laws regulating the energy sector do not specify the particular methods to be used to ensure confidentiality of commercially sensitive information, however there is no general prohibition to use public cloud.

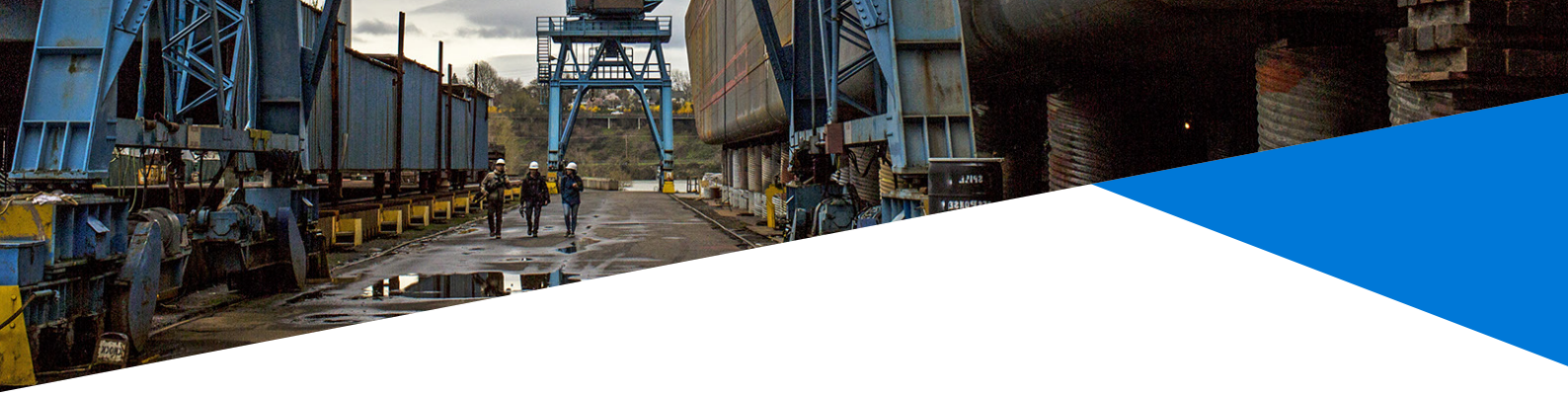
3. Legislation regarding the mining **sector** (coal, precious metals)

As required under the Underground Resources Act, the authorisation and concession holders have strict reporting and documenting obligations. In particular, such undertakings must: keep full and detailed documentation of the geological surveys and other activities related to the granted rights, and provide it for inspections pursuant to the terms of the concluded contracts; report the results from geological surveys and other activities related to the granted rights; submit to the Minister of Energy the obtained material evidence after completion of the respective research work; collect, identify, store and document information about the mineral diversity in the respective areas and facilities.

Throughout the term of validity of the authorizations and the concessions, the above information and documentation is shared property of the Minister of Energy and the authorization or concession holder. The co-owners must ensure the confidentiality of information in the course of its collection, storage, delivery and use as provided for in the respective contract concluded between them. After the expiry of the authorization or concession, this information becomes the sole property of the Bulgarian State, and the respective information must be delivered to the National Geological Fund by the authorization or concession holders.

Neither Bulgarian legislation, nor the templates for contracts used for such authorizations and

[15] Transposes Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC and Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC



concessions as typically drafted by the Bulgarian State specify the technical methods to be used to ensure confidentiality of the above categories of information. As such, there is no general prohibition on use of public cloud for this purpose.

4. Legislation regarding the utilities sector (water)

The Water Supply and Sewage Services Act and the Waters Act are the main pieces of legislation concerning water-related services. They establish the requirements for providing water-supply and sewerage services and the legal framework for the regulation of prices, accessibility and quality of such services provided by the water-supply and sewerage service utility enterprises, under the control of the Energy and Water Regulatory Commission. "Water-supply and sewerage services" include the services of treatment and delivery of water intended for drinking and household uses, industrial uses and other uses, of drainage and treatment of waste water and rain water in urban areas, as well as the activities of construction, maintenance and operation of the water-supply and sewage systems, including the treatment plants and the other facilities.

Pursuant to the Water Supply and Sewage Services Act, water-supply and sewerage service utility enterprises must carry out their activities in compliance with business plans approved by Energy and Water Regulatory Commission. The business plans cover the manufacturing, repair, investment and social programs of the utility enterprises for five-year periods. The water-supply and sewerage service providers must keep detailed information on the performance of the business plans at the disposal of the Energy and Water Regulatory Commission for a period of 10 years following the expiry of the plan.

The laws regulating the utilities sector concerning water-related services do not impose specific requirements related to the means of ensuring safe retention of the respective information by the utility enterprises. There is no general legal prohibition on the use of public cloud in this sector.

5. Legislation regarding critical infrastructures

The Bulgarian legal regime of critical infrastructures is established in the Disaster Protection Act, and its implementing legislation[16][17]. It defines "Critical infrastructure" as a system or parts thereof, which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant negative impact on the Republic of Bulgaria as a result of the failure to maintain those functions. "European critical infrastructure" ("ECI") refers to critical infrastructures, located on the territory of the Republic of Bulgaria the disruption or destruction of which would have a negative impact on at least two European Union Member States. Potential ECIs are designated as ECIs subject to the agreement of the potentially affected Member States.

The Disaster Protection Act provides that the information on designation of a specific

[16] the Ordinance on the procedure, manner and competent authorities for identification and risk assessment of critical infrastructures and their sites, and the Ordinance on the procedure for identification and designation of European critical infrastructures and the measures for their protection

[17] The Disaster Protection Act and the ECI Ordinance transpose the requirements of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

infrastructure as ECI, the operator security plan, and any information communicated from the ECI operator / owner to the minister responsible for the respective sector must be treated as classified information in compliance with the requirements of the Classified Information Protection Act, subject to an appropriate level of classification.

6. Legislation regarding classified information

Classified Information Protection Act defines "classified information" as any information which is a State secret or an official secret, and any foreign classified information. Access to information that is classified as State secret may be granted only to persons that have received access authorisation on a "need-to-know" basis and subject to appropriate background checks.

Information the unauthorized access to which might threaten or damage the interests of Bulgaria relating to national security, defense, foreign policy or the protection of the constitutional order is classified as State secret, in accordance with the respective list of categories of information under the Classified Information Protection Act. There are three types of State secrets, differentiated with different types of mandatory marking depending on the risk associated with potential unauthorized access to such data: "Top secret", "Secret", and "Confidential". Information could be classified as official secret only where specified by law – the relevant marking is "For Official Use Only".

The Classified Information Protection Act imposes specific obligations with respect to the usage of communication and information systems ("CIS") for storage of classified information. It is only permissible to generate, process, store, or transmit classified information in a CIS that has received a certificate from The State Agency for National Security. Furthermore, there are additional legal restrictions with respect to the interconnection of such certified CISs. Most notably, a CIS designed for classified information of the "Top Secret" level may not be interconnected at all, even with other certified systems. In that regard, there would be regulatory difficulties related to the usage of a cloud service for storage of information classified as State secret, and it would be outright impossible to do so with respect to data classified as "Top Secret".

7. Conclusions

Bulgarian power, mining and utilities laws, including the rules on critical infrastructures, do not contain any general prohibition on cloud usage.

The reviewed Bulgarian laws contain various confidentiality and data retention requirements that may be complied with by using public cloud. The usage of public cloud regarding national and European critical infrastructure, as well as the reviewed sectors in general, must comply with applicable rules on classified information. A regulatory blocker on the usage of cloud services exists with respect to State secrets of the "Top Secret" level.

Croatia

1. Analysis

1.1 Rules applicable to public sector bodies involved in critical infrastructure

The Law on State Information Infrastructure prescribes the rights, obligations and responsibilities of competent PS bodies regarding the establishment, development and management of the state information infrastructure system, the establishment and management of the public registries system and the conditions that the state information infrastructure must provide in relation to public registries, including the PS bodies involved in the Critical Infrastructure.

Amongst other requirements, the Law on State Information Infrastructure explicitly prescribes that public registries[18] must be stored in data centres located in the territory of Croatia. Therefore, use of Cloud (including public Cloud), which involves storing of public registries in data centres located outside Croatia (including EU), is not possible under the currently applicable law. Thus, this legal solution represents a **direct blocker** to storing or transporting public registries outside Croatia.

This applies to any public registries kept by the competent PS authorities involved in/related to the Critical Infrastructure. E.g. Regulation on Manner of Establishment, Content and Keeping the Registry of Investment[19] prescribes keeping of the registry of investments in the energy sector, which falls under said requirement of local storage. Equally, the Law on Gas Market (Article 145), envisages the obligation of the Ministry of Economy of keeping various registries related to exploration and exploitation of mineral resources, that fall under said localization requirements.

Moreover, the Regulation, which has been adopted on the basis of the Law on State Information Infrastructure, envisages the establishment of the Shared Services Centre (SSC) that will provide different IaaS, PaaS, SaaS and CaaS services to the PS bodies, through the model of a private, State-owned and managed Cloud. The exact scope of services to be provided by SSC shall be determined subsequently in a Catalogue adopted

[18] Defined in Article 2, paragraph 1, Point 10 of the Law on State Information Infrastructure as: "official records kept in electronical form, consisting of structured, arranged, mutually connected and synchronized data about the subject of registration into the registry and data which are related to the subject of registration, within the area of competence of the public sector bodies, and which has been established and is kept based on the law or international treaty, and which serves for collection and storage of data within the prescribed performance of the duties of the public sector bodies".

by competent authorities, while the minimum services to be provided are listed in Article 9 of the Regulation. According to our findings, the same Catalogue has not yet been adopted or published.

The Regulation envisages that the technical infrastructure of the SSC will "primarily" be established in the territory of Croatia, while the competent authorities will determine the criteria for storage of data in data centres on the territory of the Republic of Croatia, as well as for which data the use of public Cloud on the EU territory will be allowed. Based on the information available to us, such criteria have not yet been adopted or published. The service providers to the SSC as listed in the Regulation (envisaged as the State's partners in establishing of the SSC), shall provide services to the SSC either by their own means, or through services procured on the market.

PS bodies, including those involved in Critical Infrastructure sectors, are legally obligated to use the services of the SSC, as listed in Article 9 of the Regulation. SSC is intended for using the services that are connected with the data of degree of secrecy of classified data of class "non-classified" and "restricted" (hereinafter: **"Non-classified data"**), and it shall not provide services for data that are of degree of secrecy of classified data of class "confidential", "secret" and "top secret" (**"Classified data"**)[20].

Article 12 of the Regulation, states that the State Information Infrastructure (integral part of which should be SSC) is non-classified, and that the adequate measures and standards determined in the regulations on information security apply to the same. In line with the Law on Information Security (Article 6), measures and standards of information security for protection of non-classified data are determined in line with measures and standards legally prescribed for protection of personal data of citizens, i.e. those established by the GDPR and local GDPR implementation law.

It is expected that the SSC will become operational in the next three years. According to the information available to us, it appears that it is planned to include first 40 PS bodies in the SSC by the end of this year, while approximately 300 PS bodies should be included once the SSC becomes fully operational.

The introduction of the SSC by the Regulation imposes several **direct and indirect blockers** to use of public Cloud and/or storage of Non-classified data outside Croatia (which blockers apply in addition to the requirement of keeping the public registries locally as elaborated above), as follows:

- First, SSC is envisaged as a private State-owned and managed Cloud for providing of particular IaaS, PaaS, SaaS and CaaS services to the PS. Since SSC is envisaged as a private Cloud, primary use of public Cloud for the purposes of SSC is excluded, and any use of a public Cloud would be delegated to the secondary role;
- Second, PS bodies are obligated under the law to use IaaS, PaaS, SaaS and CaaS services of SSC as listed in Article 9 of the Regulation. Therefore, procuring the same services on the market, independently from SSC and the legally designated service providers to SSC, is not permitted for the PS bodies. This includes different data storage services listed in the same Article 9 of the Regulation;
- Third, it is envisaged in the Regulation that the technical infrastructure of the SSC shall be established "primarily" on the territory of

Croatia. Although, such wording allows for establishment of the technical infrastructure also outside the territory of Croatia, we believe that in practice, the relevant provision will likely be interpreted to restrict the location of the technical infrastructure on the Croatian territory;

- Fourth, it is prescribed in the Regulation that the competent authorities will subsequently determine the criteria for storage of Non-classified data in data centres on the territory of the Republic of Croatia, as well as for which data the use of public Cloud on the EU territory will be allowed. Until the competent authorities determine such criteria, both the service providers to the SSC, as well as the PS bodies are in no position to procure any services on the market concerning such storage.

Classified data is generally exempted from use in the public Cloud and/or transferring/storing outside Croatia, pursuant to the provisions of the Law on Information Security and the related Regulation on Information Security Measures.

It is questionable whether these legal restrictions and Non-classified data localization requirements established by applicable Croatian laws and regulations are completely in line with the current EU regulations and initiatives concerning the free flow of data. Especially, since the SSC and the technical infrastructure of the PS is envisaged for Non-classified data, for which the same standards of protection as prescribed by law for personal data should apply. The GDPR has confirmed the free flow of personal data across the EU, and now the same has been made for non-personal data through the Regulation on Free-Flow of Non-personal Data. It is therefore to be seen whether such localization requirements may be justified by the reasons of public safety, in particular taking into the consideration that under the Regulation on Free-Flow of Non-personal Data, free flow of non-personal data may be restricted only for the genuine and serious reasons of public safety.

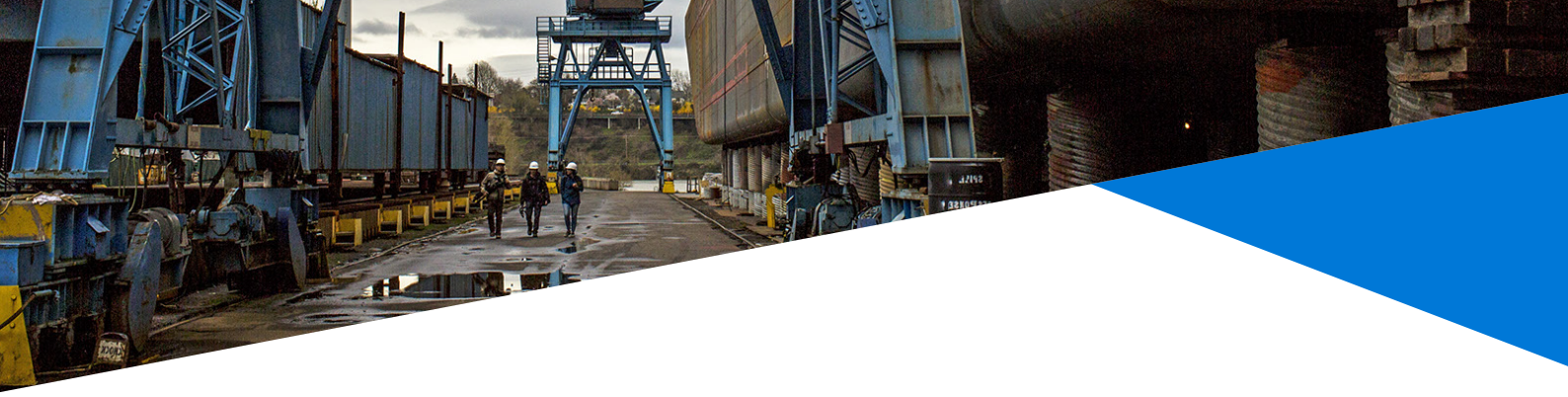
1.2 Electricity sector

The electricity sector and the information managed within the same is governed by the Law on the Electric Energy Market[21], and a number of regulations adopted on the basis on the same law. The Law on the Electric Energy Market sets forth general rules for confidentiality of the information managed in this sector. Pursuant to Article 9, transmission and distribution system operators, operators of the electric energy market, supply undertakings, traders and producers, as well as the Croatian Energy Regulator Agency[22] are obligated to preserve confidentiality of commercially sensitive information obtained in the course of carrying out their activities, from other subjects and buyers, unless they are obligated to disclose such information under the law.

Moreover, under the same Article 9 of the Electric Energy Market, transmission system operator and transmission system owner are required to preserve confidentiality of commercially sensitive information obtained in the course of carrying out their activities and shall prevent information about their own activities which may be commercially advantageous from being disclosed in a discriminatory manner. In particular they shall not disclose any commercially sensitive information to the remaining parts of the undertaking, unless this is necessary for carrying out a business transaction.

Furthermore, in order to ensure the full respect of the rules on information unbundling, the transmission system owner and the remaining

[21]("Zakon o tržištu električne energije") (OG no. 22/2013, 95/2015, 102/2015, 68/2018) (https://narodne-novine.nn.hr/search.aspx?upit=zakon+o+tr%C5%BEi%C5%A1tu+elektri%C4%8Dne+energije&naslovi=da&sortiraj=1&kategorija=1&rpp=10&qtype=3&pretraga=da) (hereinafter: "Law on the Electric Energy Market")
[22]("Hrvatska Energetska Regulatorna Agencija") (local market regulator)



part of its undertaking must not use joint services, such as joint legal services, apart from purely administrative or IT functions.

Equally, the transmission system operator is required to adopt, with prior approval from the Croatian Energy Regulator Agency, the program of measures for protection of confidentiality of data managed from its end. Additionally, the distribution system operator must preserve the confidentiality of commercially sensitive information obtained in the course of carrying out its business and shall prevent information about its own activities which may be commercially advantageous being disclosed in a discriminatory manner.

Additionally, the law provides for the obligation of the supply undertakings engaged to keep at the disposal of the national authorities, including the national regulatory authority, the national competition authorities and the competent EU bodies, for the fulfilment of their tasks, for at least five years, the relevant data relating to all transactions in electricity supply contracts and electricity derivatives with wholesale customers and transmission system operators.

The Law on Electric Energy Market envisages misdemeanour liability, monetary fines and protective measures of ban of performing of relevant activities for the undertakings from this sector (and their authorized representatives) who fail to comply with the confidentiality obligations imposed upon them by the same law and regulations adopted on its basis.

The concept of "confidential information" is particularly emphasized and the need to provide proper security is highlighted. Confidentiality obligations are to a certain extent additionally addressed in regulations adopted on the basis of the Law on the Electric Energy Market[23].

Nonetheless, we did not identify blockers for use of electronic systems, including use of a public Cloud within the territory of the EU, for processing of information managed in this sector, neither in the Law on the Electric Energy Market nor any regulations adopted under the same law. The latter does not apply in case of public registries and Non-confidential Data kept/processed by the PS bodies involved in this sector, as outlined earlier.

The only obstacle for using the services of the same ICT services provider may be from the obligation prescribed for independent transmission system operator in line with Article 18 of the Law on the Electric Energy Market. Under it, the independent transmission system operator shall not share IT systems or equipment, physical premises and security access systems with any part of the vertically integrated undertaking nor use the same consultants or external contractors for IT systems or equipment, and security access systems. Therefore, in case when any of the vertically integrated undertakings use the services of a particular external provider of ICT services, including Cloud services provider, the independent transmission system operator should not use the same service provider.

1.3 Natural gas sector

Natural gas sector and treatment of information managed within the same sector is regulated principally by the Law on the Gas Market[24], and a number of regulations adopted under the same law. Similar as with the Electricity sector, local laws and

[23]For example, in Articles 174-175 of the Grid Rules for Distribution System ("Mrežna pravila distribucijskog sustava"), OG. No. 74/2018 (https://narodne-novine.nn.hr/clanci/sluzbeni/2018_08_74_1539.html)
[24]("Zakon o tržištu plina") (OG no. 18/2018) (https://narodne-novine.nn.hr/clanci/sluzbeni/2018_02_18_372.html) (hereinafter: "Law on the Gas Market")

regulations emphasize the concept of "confidential information" and the need to provide proper security of the same. Nevertheless, according to our findings, the same laws and regulations do not contain blockers for use of electronic systems, including use of a public Cloud within the territory of the EU, for processing of information managed in this sector.

The Law on Gas Market establishes in Article 11 the obligation of the relevant stakeholders in this sector, in the first place transmission, storage and/or LNG system operator, and each transmission system owner, as well as the Croatian Energy Regulator Agency to preserve the confidentiality of commercially sensitive information obtained in the course of carrying out their activities, from other subjects and buyers, unless they are obligated to disclose such information under the law.

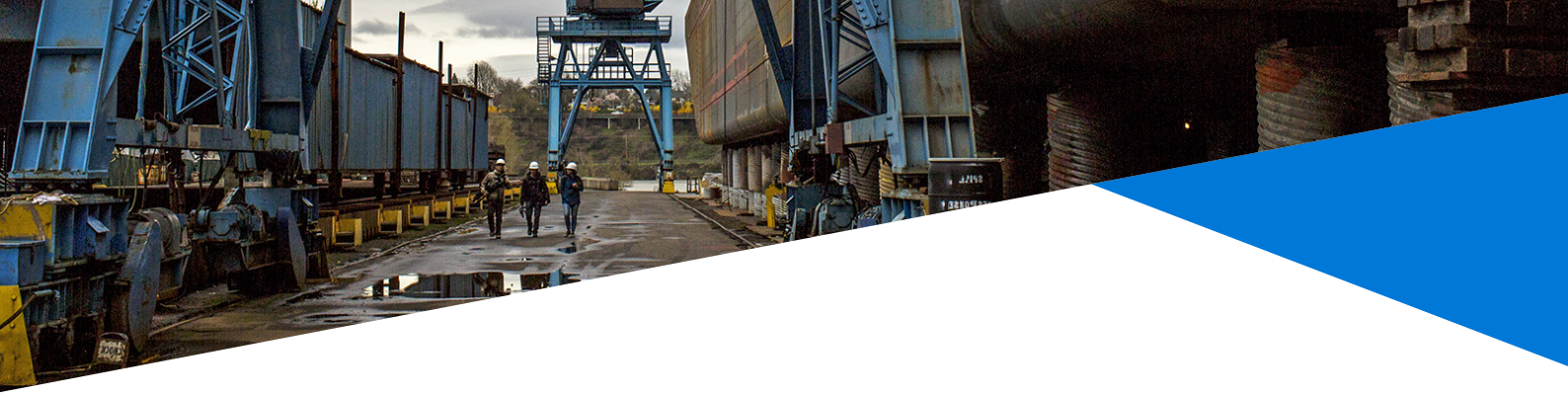
In particular, under the same Article, transmission, storage and/or LNG system operator, and each transmission system owner, are obligated to preserve the confidentiality of commercially sensitive information obtained in the course of carrying out their activities, and to prevent information about their own activities which may be commercially advantageous from being disclosed in a discriminatory manner. The same stakeholders shall not disclose any commercially sensitive information to the remaining parts of the undertaking, unless this is necessary for carrying out a business transaction.

In order to ensure the full respect of the rules on information unbundling, the transmission system owner including, in the case of a combined operator, the distribution system operator, and the remaining part of the undertaking do not use joint services, such as joint legal services, apart from purely administrative or IT functions.

Likewise, each distribution system operator shall preserve the confidentiality of commercially sensitive information obtained in the course of carrying out its business and shall prevent information about its own activities which may be commercially advantageous from being disclosed in a discriminatory manner. Distribution system operators shall not, in the context of sales or purchases of natural gas by related undertakings, abuse commercially sensitive information obtained from third parties in the context of providing or negotiating access to the system.

Additionally, the Law on Gas in said Article 11 prescribes the obligation of the natural gas suppliers to keep at the disposal of the national authorities, including the national regulatory authority, the national competition authorities and the competent EU bodies, for the fulfilment of their tasks, for at least five years, the relevant data relating to all transactions in gas supply contracts and gas derivatives with wholesale customers and transmission system operators as well as storage and LNG operators.

The Law on Gas Market envisages misdemeanour liability, monetary fines and protective measures of ban of performing of relevant activities for the undertakings from this sector (and their authorized representatives) who fail to comply with the confidentiality obligations imposed upon them by the same law and regulations adopted on its basis. The concept of "confidential information" is emphasized and the need to provide proper security is highlighted. Confidentiality obligations are to a certain extent additionally addressed in regulations adopted on the basis of the Law on the Gas Market[25].



Nevertheless, we did not identify blockers for use of electronic systems, including use of a public Cloud within the territory of the EU, for processing of information managed in this sector, neither in the Law on the Gas Market nor any regulations adopted under the same law. The latter does not apply in case of public registries and Non-confidential Data kept/processed by the PS bodies involved in this sector, as outlined earlier.

The only obstacle for using the services of the same ICT services provider may arise from the obligation prescribed for independent transmission system operator in line with Article 19 of the Law on the Gas Market. Under it, the independent transmission system operator shall not share IT systems or equipment, physical premises and security access systems with any part of the vertically integrated undertaking nor use the same consultants or external contractors for IT systems or equipment, and security access systems. Therefore, in case when any of the vertically undertakings use the services of a particular external provider of ICT services, including Cloud services provider, the independent transmission system operator should not use the same service provider.

1.4 Coal and precious metals sectors

These sectors and information managed in the two same are governed by the Law on Mining[26] and the Law on Supervision of Precious Metals Objects[27], as well as a number of regulations adopted under the same two laws. The Law on Mining envisages in Article 145 that the Ministry of Economy keeps the central information system of the mineral resources of Croatia. Keeping of the same information system, as well as different registries related to exploration and exploitation of mineral resources, which form the integral part of the same system is further elaborated in the Regulation on the Central Information System of Mineral Resources[28]. It is explicitly envisaged in the same regulation, that said Central Information System is kept in electronic form.

Based on the rules for keeping of the public registries as outlined earlier, different registries related to exploration and exploitation of mineral resources which form the part of said Central Information System of Mineral Resources, must be stored in a data centre located in Croatia.

Other than aforementioned, we did not detect further blockers for use a public Cloud within the territory of the EU, for processing of information managed in these two sectors.

[25]For example, Articles 18 and 52 of the Grid Rules for Gas Distribution System ("Mrežna pravila plinskog distribucijskog sustava"), OG. No. 50/2018 (https://narodne-novine.nn.hr/clanci/sluzbeni/2018_06_50_1004.html)
[26]("Zakon o rudarstvu") (OG no. 56/2013, 14/2014, 52/2018, 115/2018) (https://narodne-novine.nn.hr/search.aspx?upit=zakon+o+rudarstvu&naslovi=da&sortiraj=1&kategorija=1&rpp=10&qtype=3&pretraga=da) (hereinafter: "Law on Mining")
[27]("Zakon o nadzoru predmeta od plemenitih kovina") (OG no. 36/2015) (https://narodne-novine.nn.hr/clanci/sluzbeni/2015_03_36_733.html) (hereinafter: "Law on Supervision of Precious Metals Objects")
[28]("Pravilnik o jedinstvenom informacijskom sustavu mineralnih sirovina") (OG no. 52/19) (https://narodne-novine.nn.hr/clanci/sluzbeni/2019_05_52_1002.html) (hereinafter: "Regulation on the Central Information System of Mineral Resources")

1.5 Water supply

Water supply sector is principally regulated in the Law on Waters[29], and a number of regulations adopted under the same law. The Law on Waters sets forth the obligation for various subjects involved in water-related activities of keeping of different inquest registries. E.g., under Article 100 of the same law, physical persons or entities performing the activities of exploitation of sand or gravel are required to keep in the legally prescribed form the inquest register of exploitation of sand and gravel as well as to report the information from the same register to competent authorities on regular basis.

The form, content, retention periods and other details related to keeping of said inquest registers are prescribed in different implementation acts (bylaws) adopted under the Law on Waters[30]. According to the Law on Waters and the latter Bylaw on Inquest Register on Exploitation of Sand and Gravel, the inquest register on exploitation of sand and gravel may be kept in physical or electronic form. In addition, the regular reports may be submitted with the competent authorities by email or physically. The retention period for the data contained in the same inquest registry is 10 years.

Very similar requirements are prescribed for keeping of other inquest registers under the Law on Waters. Therefore, we did not detect any provisions which would represent blockers for use of Cloud based solutions for processing of information related to said registers.

Furthermore, pursuant to the Law on Waters (Articles 134-140), Croatian Waters (*Hrvatske Vode*), a public institution tasked with managing of waters in Croatia, is required to keep the "Water Documentation" consisting of several registries containing information about legal acts issued by Croatian Waters, cadastral data about waters, as well as the information about granted concessions for commercial use of waters. In addition to the physical form, under the Law on Waters, the "Water Documentation" is also kept in digital form, as part of the Information System of Protection of Environment managed by the Croatian Environment Protection Agency (which is the integral part of the wider European environmental and observation network). The latter Information System and registries that form the integral part of the same, would according to our findings, fall under the localization requirements/use of SSC as elaborated above.

Other than aforementioned, we did not detect further blockers for using public Cloud within the territory of the EU, for processing of information managed in the subject sector.

[29] ("Zakon o vodama") (OG no. 53/2009, 63/2011, 130/2011, 56/2013, 14/2014, 46/2018) (https://narodne-novine.nn.hr/search.aspx?upit=zakon+o+vodama&naslovi=da&sortiraj=1&kategorija=1&rpp=10&qtype=3&pretraga=da) (hereinafter: "Law on Waters")

[30] in relation to exploitation of sand and gravel, it is the Bylaw on Inquest Register on Exploitation of Sand and Gravel ("Pravilnik o očevidniku vađenja šljunka i pijeska") (OG no. 80/2010, 3/2014) (https://narodne-novine.nn.hr/search.aspx?upit=Pravilnik+o+o%C4%8Devidniku+va%C4%91enja+%C5%A1ljunka+i+pijeska&naslovi=da&sortiraj=1&kategorija=1&rpp=10&qtype=3&pretraga=da)

1.6 Cybersecurity requirements related to operators of essential services and digital services providers

Law on Cybersecurity for Operators of Essential Services and Digital Services Providers , and the NIS Implementation Law are the main laws in this aspect. The NIS Implementation Law imposes the obligation upon private businesses or public entities with an important role for the society and economy - Operators of Essential Services (including those from the electricity, oil and gas, as well as drinking water supply and distribution sectors that fall under the legally prescribed criteria), to take appropriate security measures and to notify serious incidents to the relevant national authority. These security measures include:

- Preventing risks: Technical and organizational measures that are appropriate and proportionate to the risk.
- Ensuring security of network and information systems: The measures should ensure a level of security of network and information systems appropriate to the risks.
- Handling incidents: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.

Such security measures and notification requirements are further elaborated in the Regulation on Cybersecurity of Operators of Essential Services and Digital Service Providers .

Although the NIS Implementation Law and the NIS Regulation prescribe in detail the security and notifications measures that the Operators of Essential Services must undertake in order to safekeep the information managed from their side, we did not identify in the same legislative acts blockers for use of electronic systems, including use of a public Cloud within the territory of the EU, for Operators of Essential Services, including those from the electricity, oil and gas, as well as drinking water supply and distribution sectors.

2. Conclusion

Based on the results of available legal research and taking into the account the applicable laws and regulations, below please find our conclusions on the subject matter.

1. We did identify direct and indirect blockers to use of public Cloud and/or storage of data managed in the Critical Infrastructure sectors outside Croatia might have some direct or indirect blockers. However, based on our findings, the same blockers refer primarily to data managed by the public (PS) bodies involved in these sectors, and not to the commercial segment of businesses.

2. The Law on State Information Infrastructure explicitly prescribes that public registries must be stored in data centres located on the territory of Croatia. Therefore, use of Cloud (including public Cloud), which involves storing of public registries in data centres located outside Croatia (including EU), is not possible under the currently applicable law. Thus, this legal solution represents a direct barrier to storing or transporting public registries (including public registries established by the law in the electric, natural gas, coal and precious metals, as well as water supply sectors) outside Croatia.

3. Moreover, the Regulation, which has been adopted on the basis of the aforementioned Law on State Information Infrastructure, envisages the establishment of the Shared Services Centre (SSC) that will provide different IaaS, PaaS, SaaS and CaaS services to the PS bodies, through the model of a private, State-owned and managed Cloud. The SSC is envisaged for processing of Non-Classified Data by PS bodies. Since the SSC is envisaged as private State-owned and managed Cloud, primary use of a public Cloud for providing of said IaaS, PaaS, SaaS and CaaS services to the PS bodies is excluded. In addition, the Regulation prescribes that the Technical Infrastructure of the SSC shall be established "primarily" on the territory of the Republic of Croatia, while the competent authorities are authorized to decide in a separate document for which Non-classified Data use of a public Cloud outside the territory of the EU will be permitted. Until competent authorities adopt such decision, PS bodies are blocked from using the public Cloud outside Croatia for storage of Non-classified data. Therefore, such legal solution which is applicable to PS bodies within subject sectors, represents both direct and indirect barrier to use of a public Cloud and/or storing Non-classified data of the PS outside Croatia. It is questionable whether these legal restrictions and Non-classified data localization requirements established by applicable Croatian laws and regulations are completely in line with the current EU regulations and initiatives concerning the free flow of data, and that is yet to be established. It should be noted that the latter legal restrictions and Non-classified data localization requirements apply in addition to the requirement of keeping the public registries locally, as elaborated above under point b).

4. Besides afore-described restrictions applicable to the PS bodies involved in electric, natural gas, coal and precious metals, as well as water supply sectors, the applicable legislation does not seem to have any further restrictions for PS or non-PS to use of a public Cloud or storage of data managed in these sectors outside Croatia, as long as such use comply with the legal security requirements.

[31]("Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga") (OG no. 64/2018) (https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html) (hereinafter: "NIS Implementation Law")
[32]National implementation act for the DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (https://eur-lex.europa.eu/legal-content/EN-HR/TXT/?uri=CELEX:32016L1148&from=HR)
[33]("Uredba o kibernetičkoj sigurnosti pružatelja ključnih usluga i davatelja digitalnih usluga") (OG no. 68/18) (https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_07_68_1399.html) (hereinafter: "NIS Regulation") which has been adopted on the basis of the NIS Implementation Law

Estonia

1. Power & utilities sector

1.1 Energy sector (electricity, coal and precious metals)

There are various laws regulating this field, but the most relevant act in relation to use of cloud services is Electricity Market Act . Electricity Market Act governs the generation, transmission, sale, export, import and transit of electricity and the economic and technical management of the power system.

The Act stipulates that the system operator[35] shall create an information exchange platform and administrate it. An information exchange platform is a digital environment for information exchange in the electricity market for the purpose of changing open suppliers, transmitting metering data, performing the obligations imposed on market participants by the law and ensuring the rights granted to them. Therefore, the system operators are obligated to create an appropriate information exchange platform, whereas the use of public cloud is not limited.

Regarding confidentiality requirements, network operators maintain the confidentiality of any information concerning the amounts of electricity generated or consumed by a market participant that it receives in the course of performing its functions.

The Act addresses the information systems and its requirements in very general terms. The use of public cloud is not explicitly addressed, and therefore it's not prohibited.

1.2 Utilities sector (natural gas and water supply)

There are multiple legal acts regulating this field, but the most relevant acts in relation to use of cloud services are Natural Gas Act[36], Water Act[37] and Public Water Supply and Sewerage Act[38].

Similarly to the Electricity Market Act, the Natural Gas Act stipulates that the system operator creates a digital environment (data exchange platform), and makes it possible, on an equal footing, for market participants who have the corresponding statutory duty and the corresponding statutory right to submit and to receive

[34]In Estonian Elektrituruseadus. Available in English: https://www.riigiteataja.ee/en/eli/520032019017/consolide.
[35]transmission network operator.
[36]In Estonian Maagaasiseadus. Available in English: https://www.riigiteataja.ee/en/eli/520032019006/consolide.
[37]In Estonian Veeseadus. Available in English: https://www.riigiteataja.ee/en/eli/526022019001/consolide.
[38]In Estonian Ühisveevärgi ja -kanalisatsiooni seadus. Available in English: https://www.riigiteataja.ee/en/eli/506072018002/consolide.

data. The use of a cloud service is not limited.

In general, the Natural Gas Act, Water Act and Public Water Supply and Sewerage Act do not contain many requirements for the information systems. The use of public cloud is not explicitly addressed, and therefore it's not prohibited.

2. Legislation regarding cybersecurity

The Cybersecurity Act[39] is an implementing act that has been adopted under the NIS Directive. Cybersecurity Act provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.

Cybersecurity Act is not applied to the processing of state secrets and classified information of foreign states or to the maintenance of processing systems for such information. If the planned use of public cloud also contains classified information, the requirements of the State Secrets and Classified Information of Foreign States Act[40] should be applied. Additionally, the ministers responsible for the area have adopted regulations, specifying the requirements to encrypted materials and processing and protection thereof[41] ; requirements for ensuring radiation safety[42] ; and requirements for computer and local networks security[43].

The Cybersecurity Act is applicable to digital service providers and service providers (including a provider of a vital service provided for in the Emergency Act[44] upon providing the vital service). Cybersecurity Act emphasizes that service providers specified in Cybersecurity Act who operate in sectors set out in Annex II to NIS Directive[45] are deemed to be operators of essential services for the purposes of NIS Directive. According to the Emergency Act a provider of a vital service is a legal person whose competence includes the fulfilment of a public administration duty defined as a vital service. Vital services are electricity supply, natural gas supply, district heating, water supply and sewerage, etc. The specific conditions to be considered a provider of a vital service are determined by law. Therefore, potentially all the requirements applicable to service providers (in addition to the requirements applicable to digital service providers) must be taken into account when considering the provision of cloud services in the power and utilities sector.

According to the Cybersecurity Act, a service provider must permanently apply organisational, physical and information technological security measures for preventing and resolving cyber incidents and for preventing and mitigating an impact on the continuity of the service or the security of the system due to a cyber incident or for preventing and mitigating a possible impact on the continuity of another dependant service or the security of a system. Upon the application of security measures, the service provider is required to prepare a system risk assessment, ensure the monitoring of the system for detecting actions or software compromising its security, etc.

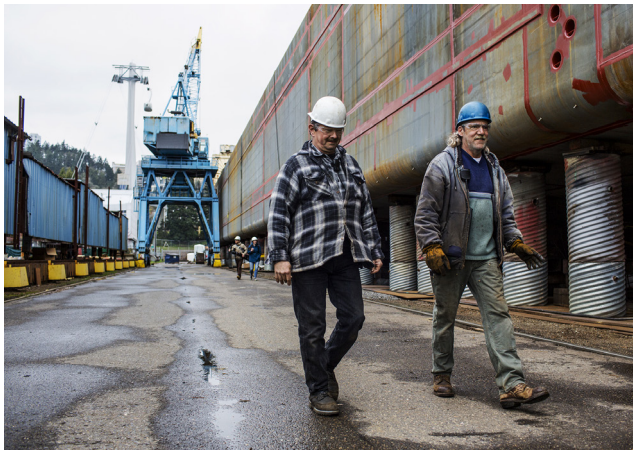
If the service provider authorises another party to administer the system or uses another party to host the system, the service provider is responsible for the application of the security measures of the system by the other party. The description of the security measures of the system used for the provision of a service and the requirements for the preparation of a risk assessment are established by a regulation of the minister responsible for the area.[46]

[39]In Estonian Küberturvalisuse seadus. Available in English: https://www.riigiteataja.ee/en/eli/523052018003/consolide.
[40]In Estonian Riigisaladuse ja salastatud välisteabe seadus. Available in English: https://www.riigiteataja.ee/en/eli/501042019009/consolide
[41]Available in Estonian: https://www.riigiteataja.ee/akt/128062017048.
[42]Available in Estonian: https://www.riigiteataja.ee/akt/128062017049.
[43]Available in Estonian: https://www.riigiteataja.ee/akt/128062017064.
[44]In Estonian Hädaolukorra seadus. Available in English: https://www.riigiteataja.ee/en/eli/525062018014/consolide.
[45]Annex II to NIS Directive lists the following sectors: Energy, Transport, Banking, Financial market infrastructures, Health sector, Drinking water supply and distribution, Digital Infrastructure. The subsectors and types of entities are also specified in Annex II. The NIS Directive and the Annex II are available in English: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148#.
[46]Available in Estonian: https://www.riigiteataja.ee/akt/110072018006.

The Cybersecurity Act also stipulates security measures of digital service provider's system. In choosing measures for ensuring the security of a system the security of the technical infrastructure, the prevention, detection and resolution of a cyber incident; continuity management; monitoring, auditing and testing; and compliance with international standards must be taken into account. Therefore, the Cybersecurity Act does not directly regulate the use of cloud services, and therefore its use is not prohibited. However, all security requirements must be taken into account when providing a cloud service. All the aforementioned requirements are further explained in the Explanatory Memorandum to the draft act of the Cybersecurity Act.

The Emergency Act stipulates that if information systems ensuring the operation of a vital service are located in a foreign country, the provider of the vital service is also required to ensure the continuity of the vital service in a manner and by means not dependent on information systems located in foreign countries.

According to the Cybersecurity Act, state supervision over the compliance with the requirements set for digital service providers is exercised if the Estonian Information System Authority is notified of said requirements not being complied with by a digital service provider established in



Estonia; a digital service provider belonging to a group whose parent company is established in Estonia; or a digital service provider of a third country who has a representative in Estonia.

3. Conclusion

Having researched and analysed the legislation applicable to the sectors referenced herein, we are of the opinion that there are no statutory prohibitions for the use of public cloud for companies in these sectors in Estonia. We advise that this conclusion should be read along with the above analysis for complete reference.

Latvia

1. Power & utilities sector

1.1 Energy sector (electricity, gas and heating)
There are several laws governing the energy sector in Latvia, and its overall regulation is established by the Energy Law[48]. The law, among other things, regulates the energy industry as the economic sector and it covers such matters as acquisition and use of energy resources for the production of various types of energy.

The Energy Law is silent on the use of public cloud and therefore we believe that use of public cloud is allowed, but the law contains several general obligations for the entities operating in the energy sector. The Energy Law states[49] that it is the duty of the energy supply entities to ensure continuous operation of their objects and appropriate technical condition of these objects. In order to ensure safe and effective operation of the inter-connected energy supply systems, the energy supply entities are allowed[50] to mutually exchange the necessary information at the same time ensuring protection of commercial secrets. The law also contains an obligation for the operators of energy systems to ensure that additional services used by the operators for maintenance of the system are performed by such service providers that are able to perform the services at the required quality and for the lowest possible costs. At the same time the stability and safety of the system has to be maintained.

Additionally, the operations of the entities supplying energy are governed by the law "On Regulators of Public Utilities"[51] and Electricity Market Law[52]. None of the two laws specifically address the use of cloud services. The law "On Regulators of Public Utilities" deals mainly with the procedures on licencing of the different energy market participants and it also applies to providers of other public utility services, e.g., postal services, heating and water supply, waste collection.

[47]Available in Estonian: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59.
[48]In Latvian Enerģētikas likums. Available in English: https://likumi.lv/ta/en/en/id/49833-energy-law
[49]The Energy Law, article 9
[50]The Energy Law, article 14
[51]In Latvian likums "Par sabiedrisko pakalpojumu regulatoriem". Available in English: https://likumi.lv/ta/en/en/id/12483-on-regulators-of-public-utilities
[52]In Latvia Elektroenerģijas tirgus likums. Available in English: https://likumi.lv/ta/en/en/id/108834-electricity-market-law

It states[53] that providers of public utility services use and promote implementation of effective, economic and safe technologies aimed at maintenance and improvement of the quality of the provided utility services.

The Electricity Market Law establishes rules for operation of electricity supply market in Latvia and lays down different obligations mostly of technical nature to ensure that electricity supply is safe and uninterrupted, and that the market is available for different sellers of the electricity. Similarly, as in Estonia, also in Latvia the Electricity Market Law provides for operation of an electricity trading platform (electricity exchange) managed by the electricity market operator. According to the law the electricity exchange is an electricity trading platform in Latvia, where participants of the electricity exchange buy and sell electricity (trade of electricity also includes the physical transmission of electricity). The Regulator of Public Utilities appoints the electricity market operator and monitors its operations, taking into consideration the applicable EU regulation.

With respect to handling of information the law obliges all operators to provide for confidentiality of the information that the operator receives from other participants of the electricity market in the course of performance of its operations. To strengthen this duty, the law grants the Regulator of Public Utilities to impose a fine on transmission system operator and distribution system operator in the amount of 10% of the annual turnover for breach of confidentiality with respect to information received from other market participants.

1.2 Utilities sector (gas, heating and water supply)

The utilities sector is mainly governed by the Energy Law described in the previous section, except for water management systems which is governed by the Law on Water Management Services[54].

Similarly, as to other laws, the law does not address the issue of cloud services and therefore we believe that use of public cloud is allowed, and it mainly consists of general duties and obligations of the water management service providers and users and therefore we believe that use of the public cloud is allowed also in this sector.

There are a number of Cabinet of Ministers regulations and Regulations adopted by Regulators of Public Utilities with respect to provision of utility services to consumers, but they are mostly of technical nature or address the issues of pricing of the utility services. With respect to processing of information some of them repeat the duty to protect personal data and information containing commercial secret that has been disclosed to the service provider, but there is no further regulation about use of cloud services.

2. Legislation regarding cybersecurity

Since 2011, the Law on Security of Information Technologies[55] is effective in Latvia and it is the implementation act of the NIS Directive. Its purpose is to improve the security of information technologies by laying down the most important requirements in order to guarantee the receipt of essential services which are supplied by use of the above referred technologies. The requirements of this law are binding for state and municipal institutions, as well as for commercial entities and other legal entities.

The law specifically addresses the issue of critical infrastructure of IT technologies which is approved by the Cabinet of Ministers[56] . The critical infrastructure is protected in order to ensure performance of basic functions essential for state and society. The Cabinet of Ministers adopted special regulations[57]with respect to the security

[53]Law "On Regulators of Public Utilities", Article 22
[54]In Latvian Ūdenssaimniecības pakalpojumu likums. Available in English: https://likumi.lv/ta/en/en/id/275062-law-on-water-management-services
[54]In Latvian Informācijas tehnoloģiju drošības likums. Available in English: https://likumi.lv/ta/en/en/id/220962-law-on-the-security-of-information-technologies
[56]Law on National Security. In Latvian Nacionālās drošības likums. Available in English: https://likumi.lv/ta/en/en/id/14011-national-security-law
[57]In Latvian Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība. Available in English: https://likumi.lv/ta/en/en/id/212031-procedures-for-the-identification-of-critical-infrastructure-including-european-critical-infrastructure-and-planning-and-implementation-of-security-measures

measures applicable to the critical infrastructure of IT technologies and the order of planning and implementation of such infrastructure measures[58]. The regulations do not contain any provisions regarding cloud services and it can be assumed that the use of public cloud in this sector is allowed.

The Law on Security of Information Technologies contains definitions for a) providers of basic service, b) providers of digital service, and c) representative of the digital service provider. The provider of basic service is defined as state or municipal institution or private legal entity that performs its commercial activity in Latvia and offers the following services:

1. financial services, and financial market infrastructure services, drinking water supply or distribution services, internet traffic exchange services, domain name system services, top-level domain name register services or services in the energy, transport or health sector in any EU member state;
2. services provision of which depends on information technologies, and
3. service provision of which can be substantially and negatively impacted by IT security incident.

Further, the provider of digital services defined as a private legal entity corresponding to one of the two criteria:

1. it performs commercial activity in the territory of the Republic of Latvia and offers online trading, online search engine and cloud computing services in an EU member state, or
2. it performs commercial activity outside the territory of the European Union and the digital services are offered in Latvia and provided via authorised representative.

The law sets the conditions for determining the materially disruptive impact of an information technology security incident, the procedure for requesting information from private legal persons, as well as the conditions for granting, reviewing and terminating the status of the basic service provider and the basic service, and the procedure for informing the Digital Security Monitoring Committee of the basic services providers.

The respective regulations of Cabinet of Ministers[59] , adopted in January 2019, establish the order of evaluation of the security incident and gathering of information, as well as provisions on granting, review and termination of status of basic service and status of provider of basic services.

The law defines IT security incident as a harmful event or action resulting in threat to integrity, availability and confidentiality of information technologies. It formulates the activities to be performed by the entity impacted by the IT security incident. Mainly these activities can be characterised as following the instructions issued by the institutions responsible for eliminating of security incidents; in case of substantial incidents there is an additional duty to immediately inform the institutions. The regulations of Cabinet of Ministers[60] regulates the criteria for classification of the security incident, order of informing and the report's contents.

The law also contains guidelines for activity in case a system security vulnerability is identified, and the system vulnerability is defined as essential systemic weakness that is caused intentionally or unintentionally during establishment, maintenance or modification of an information system or electronic communications network, as a result of which the integrity, accessibility or confidentiality of information technologies may be endangered. Once the

[58]This order is established by Cabinet of Minister Regulations No 496 of 01 June 2010. Regulations establish the obligations of the state and municipal institutions in formation and work of the inter-institutional commission for national security that is responsible for identification of critical infrastructure and monitoring the security and safe operation of such infrastructure.

[59]In Latvian Noteikumi par nosacījumiem drošības incidenta būtiski traucējošās ietekmes noteikšanai un kārtību, kādā piešķir, pārskata un izbeidz pamatpakalpojuma sniedzēja un pamatpakalpojuma statusu. Text available here: https://likumi.lv/ta/id/304327-noteikumi-par-nosacijumiem-drosibas-incidenta-butiski-traucejosas-ietekmes-noteiksanai-un-kartibu-kada-pieskir-parskata-un-izbe... Translation to English is not yet available.

[60]In Latvian Noteikumi par drošības incidenta būtiskuma kritērijiem, informēšanas kārtību un ziņojuma saturu. Text available here: https://likumi.lv/ta/id/304284-noteikumi-par-drosibas-incidenta-butiskuma-kriterijiem-informesanas-kartibu-un-zinojuma-saturu Translation to English is not yet available.

vulnerability is established the owner of the critical IT infrastructure or respective state and municipal institution is granted 90 days to eliminate the problem, but identification of the vulnerability has to be immediately reported to the respective institution responsible for eliminating of security incidents.

With respect to management of security of IT the head of entity (state, municipal institution, as well as owner of the critical IT infrastructure, provider of basic service and provider of digital service) is responsible for information technology security management. To this end, the head of the institution appoints the responsible person and this person is also notified to institution responsible for eliminating of security incidents. The main responsibilities of this officer are to organise management of the IT security, to carry out regular reviews of operations of IT systems and to organise elimination of the identified problems. The responsible person also has to participate in the educational courses organised by the institution responsible for elimination of security incidents, and to educate (instruct) the employees of the respective entity on IT security matter.

Cabinet of Ministers establishes the IT security requirements for private legal entities that are providers of basic service and digital service, as well as establishes the requirements and order of complying with the requirements for state and municipal institutions, and owners of critical IT infrastructure. The respective regulations of Cabinet of Ministers[61] are effective since 2015 with amendments effective since January 2019.

3. State information systems

In Latvia the state information system is defined as a structured aggregate of information technology and databases, which ensures the proposal, creation, compilation, accumulation, processing, utilisation and destruction of information (hereinafter - circulation of information) necessary for the performance of functions of the state. The key law in this area is the Law on State Information Systems[62] which aims to ensure the accessibility of information provided by the state and local municipal institutions and the quality of the state information systems. The ministry of protection of environment and regional development is coordinating the operation of state information systems. The procedures for supervising development projects for state information systems, as well as the general technical and security requirements for the information systems are governed by several Cabinet of Ministers regulations.

The Law on State Information Systems lists the main principles of operation of the state information systems. All state information systems have to be included in an integrated state information system, it is prohibited to collect the information from data subjects if such information is already available in the systems, the respective information about the data subjects has to be registered in the appropriate information system and the information has to be updated. The manager of state information system can provide for exchange of information between the state information system and the information that is collected in the databases owned by private entities.

[61] In Latvian Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām. Available in English: https://likumi.lv/ta/en/en/id/275671-procedures-for-the-ensuring-conformity-of-information-and-communication-technologies-systems-to-minimum-security-requirements
[62] In Latvian Valsts informācijas sistēmu likums. Available in English: https://likumi.lv/ta/en/en/id/62324-law-on-state-information-systems

The manager of state information system is obliged to implement the processes how to identify the information at any stage of circulation of the information. To protect the information from unauthorised access the manager of the state information system has to ensure that all system users are identified and are granted with appropriate access rights to the information system.

Although all state information systems are property of the state, the law allows that resources for information technology and information transmission that ensure operation of the state information system, may be public or private property. The state information system manager has to ensure conformity with the requirements for security of the state information system specified in the laws and regulations. The information system manager has to appoint a security manager who is responsible for management of security of respective information system.

There exists a state information systems' integrator which is a centralised aggregate of information technologies, with the assistance of which the circulation of information may be ensured within the scope of the state information system, as well as between state information systems and other information systems that are established and maintained by state or local government institutions or private individuals. The law requires that the activities of the state information systems' integrator ensures the circulation of information according to a number of criteria described in the law. For example, the activities of the integrator has to ensure such level of security of the circulation of information, which is similar to the level of security when ensuring the circulation of information without a State information systems' integrator.

4. Conclusion

Having researched and analysed the legislation applicable to the sectors referenced herein, we are of the opinion that there are no statutory prohibitions for the use of public cloud for companies in these sectors in Latvia. We advise that this conclusion should be read along with the above analysis for complete reference.

Lithuania

1. Power & utilities sector

1.1 Energy sector (electricity, gas and heating)
There are a number of legal acts governing the energy sector in Lithuania. The overall regulation of the energy sector is established in the Law on Energy[63]. The law establishes the main aims of energy activities in Lithuania as well as the legal basis of state management, regulation, supervision and control of the energy sector, the general criteria, conditions of and requirements for public relations, and the main areas of state energy policy.

The Law on Energy does not establish provisions on the use of public cloud, but it contains several general obligations for the entities operating in the energy sector. In Article 31 of the Law on Energy it is established that energy undertakings engaged in the activities of supply of energy or energy sources shall store for not less than five years and provide to competent state authorities at their request data on all their transactions with customers (excluding household customers) and transmission system operators concluded under electricity or gas supply contracts and derivative financial instruments in the electricity or gas markets. According to Article 25 of the Law on Energy, state and municipal institutions and agencies shall have the right to obtain from energy undertakings information required for the performance of their functions. Energy undertakings shall, in accordance with the procedure laid down by the Government or an institution authorised by it, provide information to state and municipal institutions, agencies and/or other persons entitled to receive such information. According to the Law on Energy, the data storage methods and instruments shall be established in accordance with the guidelines published by the European Commission (Part 4 Article 31).

Additionally, the operations of the entities supplying electricity, gas and heating are governed by Law on Electricity[64], Law on Natural Gas[65], and Law on the Heat Sector[66]. None of the three laws specifically address the use of cloud services, and therefore no prohibitions exist for use of public cloud.

[63] In Lithuanian Lietuvos Respublikos energetikos įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/cc700b403c3f11e68f278e2f1841c088?jfwid=-19kda1ip8y

[64] In Lithuanian Lietuvos Respublikos elektros energetikos įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/6a2831f0b99d11e3bda4be6f16c2da2b?jfwid=rivwzvpvg

[65] In Lithuanian Lietuvos Respublikos gamtinių dujų įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a071f720c78511e682539852a4b72dd4?jfwid=q8i88lzdy

[66] In Lithuanian Lietuvos Respublikos šilumos ūkio įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/d145d7d0b28511e8aa33fe8f0fea665f?jfwid=11dyhejazj

The Law on Electricity establishes the legislative framework for the organisation of the Lithuanian electricity sector governance, regulation, supervision, control and operations in the electricity sector, and also regulate relationship between the institutions performing regulation, supervision and control of electricity producers, service providers, consumers and the national electricity sector in the areas of electricity generation, transmission, distribution, supply and ensuring of consumers' rights and legitimate interests. Provisions on the data storage are not established in this law.

The Law on Natural Gas establishes relations in respect of natural gas transmission, distribution, storage, liquefaction and supply. The law lays down the rules relating to the organisation and functioning of the natural gas sector, access to the market, the criteria and procedures applicable to the issue of licences for transmission, distribution, storage, liquefaction and supply of natural gas and licences to undertake market operator activities. The law also defines measures to adequately safeguard security of natural gas supply and to implement the single internal market of the European Union. According to Article 24 of the law, gas supply undertakings must keep for five years and, if needed, provide data of all transactions with wholesale customers and transmission system, distribution system, storage and LNG system operators in relation to the duration of the transactions, delivery and payment terms, quantity, dates and conditions of execution, value of the transactions and measures for the identification of wholesale customers.

The Law on the Heat Sector regulates the state management of the heat sector, activities of heat sector entities, their relations with heat consumers and their interrelationship and responsibility. Provisions on the data storage are not established in this law, and therefore the use of public cloud is not prohibited.

1.2 Utilities sector (gas, heating and water supply)

The utilities sector is largely governed by the three above mentioned laws - Law on Electricity, Law on Natural Gas, and Law on the Heat Sector. The water supply issues are regulated by two separate laws, i. e. by the Law on Drinking Water Supply and Waste Water Management[67] and by the Law on Drinking Water[68]. Requirements for the management of waste are established in the Law on Waste Management[69]. Similarly, as to other laws, these laws do not address the issue of cloud services, and therefore there is no prohibition for use of public cloud.

2. Legislation regarding cybersecurity

Since 2014, the Law on Cyber Security[70] is effective in Lithuania. The law establishes cyber security principles, specifies institutions which develop and implement cyber security policy, defines powers of such authorities in the field of cyber securities, and determines duties of cyber security entities as well as inter-institutional cooperation. The law does not apply to trust service providers which are subject to the requirements laid down in Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Critical information infrastructure means a communications and information system or part of it, a group of communications and information systems the occurrence of a cyber incident in which might have a major negative impact on the national security, economy of the country, and interests of the state and the public. The Government of Lithuania approves the methodology for

[67]In Lithuanian Lietuvos Respublikos geriamojo vandens tiekimo ir nuotekų tvarkymo įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.337310?jfwid=rivwzvpvg

[68]In Lithuanian Lietuvos Respublikos geriamojo vandens įstatymas. Available only in Lithuanian:

[69]In Lithuanian Lietuvos Respublikos atliekų tvarkymo įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ecccf681441b11e68f45bcf65e0a17ee?jfwid=q8i88lai9

[70]In Lithuanian Lietuvos Respublikos kibernetinio saugumo įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ceb0e7b291ad11e8aa33fe8f0fea665f?jfwid=-g0zryzvc8

identification of critical information infrastructure and the list of critical information infrastructure and its managers. The Government of Lithuania approves:

- the National Cyber Security Strategy;
- the institutional composition of the Cyber Security Council;
- organisational and technical cyber security requirements imposed on cyber security entities;
- National Cyber Security Management Plan.

The Government supervises cyber security crisis management as well. Important powers in the field of cyber security and in the implementation of critical information infrastructure belong to the Ministry of National Defence.

The Ministry of National Defence is responsible for the coordination of the preparation of the National Cyber Security Strategy and submission of it to the Government for approval. The Ministry of National Defence submits to the Government National Cyber Incident Management Plan and organisational and technical cyber security requirements imposed on cyber security entities for approval.

It shall be noted that critical information infrastructure is managed by the manager of the critical information infrastructure. According to Article 12 of the Law on Cyber Security, managers of critical information infrastructure:

- approve plans on cyber incident management in critical information infrastructures and submit them to the National Cyber Security Centre;
- notify digital service providers of negative impact on the operation of critical information infrastructure which resulted from malfunctioning of communications and information systems of digital service providers in accordance with the procedure established in the National Cyber Incident Management Plan;
- no less than once a calendar year test the functioning of measures intended for the management of cyber incidents in critical information infrastructures and supply the results of testing to the National Cyber Security System in accordance with the procedure established in the description of organisational and technical cyber security requirements imposed on cyber security entities;
- provide conditions for the National Cyber Security Centre to implement and control technical cyber security measures in critical information infrastructure and to put technical measures into use with the aim to measure the resistance of critical information infrastructure to cyber incidents.

Specific obligations have entities which control and/or manage the state's information resources. They must provide[71] conditions for the National Cyber Security Centre to implement and control technical cyber security measures in the state's information resources and to put technical measures into use with the aim to measure the resistance of the state's information resources to cyber incidents.

It shall be noted that energy companies, as well as other companies and organization, which manage the infrastructure applicable to power and utilities, can be recognized as managers of critical information infrastructure. Critical information infrastructure is established in accordance with the Methodology for Identifying Critical Information Infrastructure, approved by the Government of the Republic of Lithuania on 5 December 2018[72].

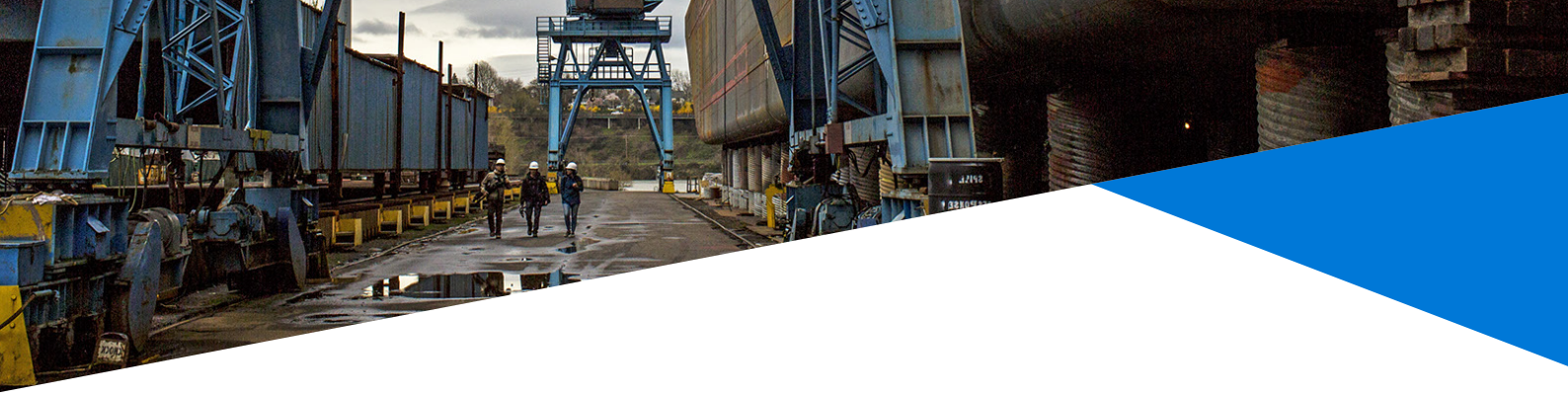
3. State information systems

In Lithuania the state information system means the entirety of legal, organisational, technical and software measures processing information necessary for the state institution (institutions) or the state agency (agencies) to perform their functions provided for in the legal acts, except for internal administration. The key law in this area is the Law on Management of State Information Resources[73] the purpose of which is to ensure proper creation, management, disposal,

[71] Law on Cyber Security, Part 2, Article 12

[72] In Lithuanian language Ypatingos svarbos informacinės infrastruktūros identifikavimo metodika, available in Lithuanian language at: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e16e7761fc4b11e89b04a534c5aaf5ce?jfwid=q8i88m9wc

[73] In Lithuanian Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. Available in English (however, be mindful that updated version is available only in Lithuanian): https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.432270?jfwid=q8i88m9d4



use, supervision, interaction, planning, financing, and protection of the state information resources. Ministry of National Defence establishes the policy in the field of state information resource security and:

- develops information security requirements, guidelines for the safety of the content of the documents;
- establishes the criteria for the assessment of the importance of information, the classification of state information systems, registers and other information systems according to the importance of the information processed therein and the procedure for their classification in the relevant category;
- manages the secure state data transmission network. The Minister of National Defence approves the Regulations of the Safe State Data Transmission Network and, in accordance with the criteria approved by the Government, the amount of remuneration for the use of the secure state data transmission network;
- performs other functions prescribed by laws and other legal acts of the Republic of Lithuania.

With the view of consolidation of state information resources infrastructure and optimization of its management, the cooperation takes place between all ministries and other state authorities of the country. These actions are coordinated by the Ministry of the Economy and Innovation.

The Resolution No. 1051 of the Government of the Republic of Lithuania "On Consolidation of the State Information Resources Infrastructure" dated 19 October 2016[74] (hereinafter – the Resolution) establishes that the state authorities, public bodies, public undertakings, and public organizations accountable to the Government, which form, organize, and (or) administer public registers, cadastres, departmental registers, information systems of the state, as well as relevant state information resources, will have to use the services rendered by the cloud computing service providers in developing, expanding, or modernizing the available state information resources infrastructure. State authorities and public bodies will have an obligation to use cloud services as may be required from time to time to update, extend, or modernize state information resources infrastructure, which has been independently acquired by them till now. This will be implemented through a special catalogue of cloud computing services, thus ensuring the appropriate terms and conditions for the provision of services as well as monitoring of provision of services.

4. Conclusion

Having researched and analysed the legislation applicable to the sectors referenced herein, we are of the opinion that there are no statutory prohibitions for the use of public cloud for companies in these sectors in Lithuania. We advise that this conclusion should be read along with the above analysis for complete reference.

[74]In Lithuanian Lietuvos Respublikos Vyriausybės 2016 m. spalio 19 d. nutarimas Nr. 1051 „Dėl valstybės informacinių išteklių infrastruktūros konsolidavimo". Available only in Lithuanian: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/d876a3f09d0511e68987e8320e9a5185/asr

Slovenia

1. Sectoral legislation

1.1 Energy sector (electricity, coal, natural gas)
The energy sector in Slovenia is mainly regulated by the provisions of the *Energy Act*[75] as described below. The acts, related to the energy sector, are also the *Mining Act*[76] and the Services of General Economic Interest Act[77]

(i) The Mining Act stipulates, among others, the conditions for the conduction of the search, exploration and exploitation of the minerals on the surface, underground or in the water.
(ii) The Services of General Economic Interest Act defines the organizational structure of the entities providing elemental resources to the society, such as energy supply (electricity, natural gas), water supply and communal services.

Neither Services of General Economic Interest Act or the Mining Act include provisions regarding data security and information processing.

1.2 The Energy Act

1.2.1 The Scope of the Energy Act
The Energy Act lays down the principles of energy policy, energy market operation rules, manners and forms of providing public services in the energy sector, principles and measures for achieving a secure energy supply, for increasing energy efficiency and energy saving and for increasing the use of energy generated from renewable energy sources, and lays down the conditions for the operation of energy installations, regulates the responsibilities, organization and tasks of the Energy Agency and the competences of

[75]Official Gazette of the RS, No. 17/14 and 81/15 (in Slovenian: Energetski zakon).
[76]Official Gazette of the RS, No. 14/14 – uradno prečiščeno besedilo in 61/17 – GZ (in Slovenian: Zakon o rudarstvu).
[77]Official Gazette of the RS, No. 32/93, 30/98 – ZZLPPO, 127/06 – ZJZP, 38/10 – ZUKN and 57/11 – ORZGJS40 (in Slovenian: Zakon o gospodarskih javnih službah).
[78]Article 1 of the Energy Act.

other authorities operating under this Act[78].
The Energy Act applies to the providers of energy activities (unless otherwise stipulated), amongst them electricity generation; supply of electricity, gas or heat; production, obtaining, marketing and distribution of liquid and gaseous fuels; storing of gaseous, liquid and solid fuels; production and distribution of heat for district heating and cooling (i.e. performers of energy sector activities), and also applies (unless otherwise stipulated) for economic operators performing the activity of coal, petroleum and natural gas extraction.[79]

Entities from the Energy Act, organized accordingly to the Services of General Economic Interest Act, are, in the field of electricity, electricity transmission or distribution system operators[80] and electricity market operators (providers of an obligatory state service of general economic interest).[81] The energy activities of heat distribution and distribution of other energy gases shall be carried out as services of general economic interest when a sustainable and uninterrupted supply of heat and other energy gases is in the public interest in order to meet public needs, otherwise the activities can be carried out either as services of general economic interest or market distribution.[82]

1.2.2 The Energy Agency

The Energy Agency is the national energy regulatory authority which monitors, directs and controls electricity and natural gas energy operators and carries out tasks regulating energy operators' activities in the field of heating and other energy gases, ensures the competitiveness of the energy markets and supervises the implementation of the EU legislation on electricity and natural gas markets. It is also responsible for harmonized data exchange between the energy market participants.[83]

1.2.3 Exchange of Information, Data Storage and Confidentiality

The provisions regarding exchange of information, data storage and confidentiality are ordinated in multiple sections of the Energy Act.
National authorities, the Energy Agency and other holders of public authority that collect the data from the performers of energy sector activities and other persons with reporting obligation under the Energy Act shall be obliged to ensure efficient cooperation in the exchange of information.[84] They may only be provided with data necessary to carry out the tasks under the Energy Act or other tasks in the field of energy. The data must be transferred in a manner that does not involve disclosure or communication of personal data. The Ministry of Infrastructure is harmonizing and overseeing the standardization of the above-mentioned data exchange.[85]

The power suppliers are obliged to store data on all transactions regarding electricity and gas supplies and derivative financial instruments etc. for at least five years and ensure availability of this data to the Energy Agency and other authorities for the exercise of their powers. This information can be stored in a public cloud to the extent the provisions of the Decree on Information Security in State Administration are observed, if applicable (see below point 3, also specifically points 3.2.2. and 3.2.3. regarding public cloud and data security classes). Afterwards,

[79]Article 6 of the Energy Act.
[80]Definition by the Article 4 of the Energy Act: a natural or legal person who carries out the function of electricity distribution system operator and is responsible for operating, maintaining and developing the electricity distribution system in a given area.
[81]Articles 35, Paragraph 3 and 36, Paragraph 20 of the Energy Act.
[82]Article 284, Paragraph 2 of the Energy Act.
[83]Articles 383 – 385 of the Energy Act.
[84]Article 33, Paragraph 1 of the Energy Act.
[85]Article 33, Paragraphs 2 and 3 of the Energy Act.

the Energy Agency shall specify the type of information that may be disclosed to market participants; the commercially sensitive information shall not be released.[86]

1.2.4 Reporting to the Energy Agency

The performers of energy sector activities must also provide all the relevant data to the Energy Agency on its request if it is necessary for the performance of administrative tasks, market monitoring and other Energy Agency's tasks, including the information that is designated as business secret.[87] The method of data transfer to the Energy Agency is determined in the *Legal Act on the Method for the Submission of Data and Documents by Providers of Energy Sector Activities.* The Act explicitly allows, when possible, and when in accordance to other provisions regarding electronic operations, automatic data exchange and processing between entities. The entities can access the information database through secure authentication log-in.[88]

1.2.5 Access to the Information

The Energy Agency shall enable access to the information to household customers consuming electricity or natural gas, regarding their rights, valid regulations, supply offers and their complaints or a dispute with a power supplier. The data in this case is also communicated in an electronic manner[89] , the method of which is prescribed in the *Legal Act Concerning the Method of Electronic Data Reporting for Valid Regular Tariffs Comparison of Electricity and Natural Gas Suppliers for Household and Small Business Customers.*[90] Liable entities must be registered in order to access the Energy Agency's electronic services. The structure and type of data is defined by the Agency's web forms or by definition of internet service for automatic data exchange and processing.[91]
The sets of data that the Energy Agency needs for the purposes of market monitoring operations, must be submitted by the performers of energy sector activities to the Energy Agency free of charge (i.e. operators, electricity producers and wholesalers, suppliers to final customers, the electricity market operator) under the provisions of the Rules on the Method for the Submission of Data and Documents by Providers of Energy Sector Activities for the purpose of Energy Agency's market monitoring.

The Energy Act extensively regulates security of data in terms of data processing, data protection, reporting etc., and in this manner in several aspects prescribes use of electronic systems. As such, it does not specifically regulate or limit the use of cloud systems.

1.3 Precious metals' sector

The *Precious Metal Products Act*[92], stipulates technical requirements that should be met by the precious metal products, compliance and trade of these products and supervision over products.

The responsibility of the Metrology Institute of the Republic of Slovenia is to fulfill expertise and related administrative and international tasks. The legislation regulating the precious metals includes provisions regarding data processing (such as

[86]Articles 156 and 280 of the Energy Act.
[87]Article 407 of the Energy Act.
[88]Official Gazette of the RS, No. 98/14 (in Slovenian: Akt o načinu posredovanja podatkov in dokumentov izvajalcev energetskih dejavnosti).
[89]Articles 46 and 171 of the Energy Act.
[90]Official Gazette of the RS, No. 69/14 (in Slovenian: Akt o načinu elektronskega posredovanja podatkov za primerjavo cenikov ponudnikov elektrike in zemeljskega plina za gospodinjske in male poslovne odjemalce).
[91]Article 11 of the Act Concerning the Method of Electronic Data Reporting for Valid Regular Tariffs Comparison of Electricity and Natural Gas Suppliers for Household and Small Business Customers.
[92]Official Gazette of the RS, No. 4/06 and 7/18 (in Slovenian: Zakon o izdelkih iz plemenitih kovin).

supplier details register, long term register data storage, non-disclosure of personal data). The Metrology Institute administrates the register containing precious metal product suppliers' data. Supplier's personal data from the register can only be processed for the purpose of its registration. The data is stored permanently.[93] This information can be stored in a public cloud to the extent the provisions of the Decree on Information Security in State Administration are observed, if applicable (see below point 2, also specifically points 2.2.1. and 2.2.2. regarding public cloud and data security classes).

1.4 Water supply sector

The *Decree on Drinking Water Supply*[94] which provides the rules regarding tasks in a domain of municipalities' public utility service of water supply. The managing of the water supply infrastructure, owned by municipality, is transferred from municipality to public utility service performers, unless the municipality performs the public service in the form of a public utility unit (both types of entities hereinafter as *the infrastructure manager*).[95]

The infrastructure manager is responsible for managing the water register (contains information about area water consumption, water reserves, prices, maintenance etc.), data of which must be stored for 10 years or more.[96] The Decree does not include any other provisions regarding data security and information processing. This information can be stored in a public cloud to the extent the provisions of the Decree on Information Security in State Administration are observed, if applicable (see below point 2, also specifically points 2.2.1. and 2.2.2. regarding public cloud and data security classes).

2. Information Security

The information security in the Republic of Slovenia is regulated by the Information Security Act,[97] which implements the Directive (EU) 2016/1148[98], and the Decree on Information Security in the State Administration[99] , which is deriving from Article 74.a of the State Administration Act[100].

2.1 The information security act

2.1.1 The Scope of the Information Security Act

The purpose of the Information Security Act is to achieve high level of network and information system security in the Republic of Slovenia, which are essential for undisrupted functionality of the state and substantial for maintaining key social and economic operations in the country. The personal data processing, based on the provisions of the Information Security Act, is executed in accordance with the personal data protection legislation, while the classified data and information, processed by the provisions of this act, are treated accordingly to the business secret and classified information regulations.[101]

2.1.2 Liable Entities

Liable entities under Information Security Act are:

(i) essential services providers,
(ii) digital services providers (web browsers, web markets, cloud computing, etc.) and

[93]Articles 14.a – 14.c of the Precious Metal Products Act.
[94]Official Gazette of the RS, No. 88/12 (in Slovenian: Uredba o oskrbi s pitno vodo).
[95]Article 19 of the Decree on Drinking Water Supply.
[96]Article 4 and 24 of the Decree on Drinking Water Supply.
[97]Official Gazette of the RS, No. 30/18 (in Slovenian: Zakon o informacijski varnosti).
[98]Directive (EU) 2016/1148 of the European Parliament and of the Council from 6th of July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[99]Official Gazette of the RS, No. 29/18 (in Slovenian: Uredba o informacijski varnosti v državni upravi).
[100]Official Gazette of the RS, No. 113/05 , 89/07, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14 and 51/16 (in Slovenian: Zakon o državni upravi).
[101]Article 3 of the Information Security Act.

(iii) state administration bodies managing the information systems or performing information services, essential for undisturbed functionality of the state or to ensure national security.

Essential services in this context are entities performing in the field of energy, drinking water supply and distribution, digital infrastructure, health-care, banking etc.[102] If a certain provider meets the required quality criteria, it shall be bounded by the Information Security Act. The criteria are as follows:

- a service provided is essential for preserving key social economic operations,
- providing a service depends on network and information system,
- security incident would cause a serious negative effect to delivery of a service (i.e. number of end users, dependence of a service on another key service, intensity and duration of effect, subject's market share etc.).

For the purpose of specifying essential service providers the Government of Slovenia is due to publish the list of essential services from the act, regulating standard services classification. The Government is also due to publish the List of individual essential services providers, who meet the above criteria[103].

2.1.3 Obligations of Essential Services Providers

The essential services providers must set up and maintain a documented security system, along with a managing system of continuous operations, which consists of risk assessment, risk management, essential information about their services, system back-up policy, incident protocols. If the essential services provider already has a documented security system, it shall be updated compliantly with the Information Security Act.

The essential services providers should, for the purpose of incident, risk and security management, ensure the preservation of diary log[104] about functionality of information systems for a period of 6 (six) months. The diary log is ensured in the territory of Republic of Slovenia (EU territory is allowed for digital and financial infrastructure).[105] As per our opinion duplicates of these logs may be stored outside Slovenia.

2.1.4 State Administration's Obligations

The state administration bodies have the same obligations pursuant the Information Security Act as the essential services providers regarding setting up the documented security system, and also, for the purpose of an incident, they shall ensure the diary logs about functionality of their information system in the territory of the Republic of Slovenia for at least 6 (six) months.[106] As per our opinion duplicates of these logs may be stored outside Slovenia. In both cases, in an event of an incident, the liable entities present an incident to the Computer Security Incident Response Team without unnecessary hesitation.[107]

2.2 The decree on information security in the state administration

The Decree on Information Security in the State Administration stipulates minimal common requirements for the state administration regarding public digital security. The Decree applies for state administration bodies, municipality bodies, public agencies, holders of public authorization and other entities, connected to the central information-communication system[108] , whereby the complete list of liable entities is not yet known/available.

2.2.1 Public Cloud

The use of public cloud must be approved by the Ministry of Public Administration which checks

[102]Article 5 of the Information Security Act.
[103]Article 7 of the Information Security Act.
[104]An audit trail is a fixed track or set of data that has occurred in an information system or device with a precise timestamp in the form of a diary log that enables a detailed overview of all records related to all events and all stored information from the creation of the information or information on to the current state.
[105]Article 12 of the Information Security Act.
[106]Article 17 of the Information Security Act.
[107]Articles 13 and 18 of the Information Security Act.
[108]Article 1 of the Decree on Information Security in the State Administration.

compliance of security, privacy and other specifications about public cloud service providers. Ministry also gives its consent to the text of terms of use, to which the end user may agree upon. The use of a public cloud service shall be compliant with the personal data protection, documentary and archive legislation. Storing, processing and exchange of the state administration's data with private accounts in the public cloud is not allowed. The data transfer between a private multimedia storage device and state administration's secured information system is prohibited.

2.2.2 Data Security Classes

The Decree defines that the computer services in publicly available cloud can be used only for information assets that are not classified in security classes or are classified in security classes Z1, C1 and R1. Classification of data is made according to the Appendix to the Decree on Information Security which defines security classes, measures for classification and procedures of classification. Security classes are sorted in three aspects: confidentiality (Z1-Z3), complexity (C1-C3) and availability (R1-R3). If the aspects of confidentiality, complexity and availability are not applicable, the information is not classified. The services in a public cloud cannot be used for higher security class data. As per our information, the liable entities have not yet provided due classifications.

3. Conclusion

The analysis and research about national sectoral legislation, potentially affecting cloud usage in Slovenia for the Power and Utilities sectors, indicates regulations regarding data storage, data processing, electronic data exchange and independence of information systems. The sectoral legislation in question does not specifically regulate or limit the use of cloud systems.

On the other hand, the national information security regulations may have effect in the subject area. Pursuant to the Information Security Act diary log about functionality of information systems must be ensured in the territory of the Republic of Slovenia (essential services providers, state administration). Although, as per our opinion, duplicates of these logs may be stored outside Slovenia. Services in public cloud can be used by liable entities pursuant to the Decree on Information Security in the State Administration only for information assets that are not classified in higher security classes.

Serbia (Non-EU)

1. Analysis

1.1 Energy

The Energy Law[112]is the principal law governing performance of energy-related activities in Serbia. Amongst other, such activities include a set of electricity and natural gas related activities.

When it comes to electricity, these are the following activities: (i) electricity generation, (ii) combined generation of electricity and thermal energy, (iii) electricity transmission and transmission system management, (iv) electricity distribution and distribution system management, (v) electricity distribution and closed distribution system management, (vi) electricity supply, (vii) wholesale electricity supply, and (viii) organized electricity market management.

The majority of these activities are performed in accordance with market principles (subject to certain regulatory requirements envisaged due to the respective activities' specifics and importance), but a few of them (i.e. electricity transmission and electricity transmission system management, and electricity distribution and electricity distribution system management) are regarded as so-called activities of general interest.

When it comes to natural gas, the following activities are prescribed: (i) natural gas transport and transport system management, (ii) natural gas storage and storage facility management, (iii) natural gas distribution and distribution system management, (iv) natural gas supply, and (v) public supply of natural gas. Unlike in the case of electricity, the majority of natural gas related activities are

[109]Article 41, Paragraph 5 of the Decree on Information Security in the State Administration.
[110]Articles 35 and 38 of the Decree on Information Security in the State Administration.
[111]Article 41 of the Decree on Information Security in the State Administration.
[112] "Official Gazette of the Republic of Serbia", nos. 145/14 and 95/18.

performed as activities of general interest (only the aforementioned activity of natural gas supply is performed in accordance with market principles).

Considering that a part of the energy related activities, including the aforementioned electricity and natural gas related activities, are identified by the Energy Law as activities of general interest, such activities' definition envisaged by the Law on Public Enterprises[113] should be noted. Under this law, activities of general interest are the activities prescribed as such by law in the fields of mining and energy, traffic, electronic communications, publishing of the Republic of Serbia's official journal and textbooks, nuclear facilities, arming and military equipment, usage, management, protection, governing and developing goods of general interest and goods in general use (water, roads, forests, navigable rivers, lakes, shores, spa, wild animals, protected areas and other), waste management and other fields. The activities of general interest are also communal activities and all other activities determined by law as activities of general interest. It is also prescribed that, as a part of performing the respective activities in the field of energy, services of general economic interest are provided.

Whether a particular activity is identified as an activity of general interest is relevant because, amongst other reasons, only certain types of entities can perform such activities. Specifically, such entities are (i) public enterprises[114], (ii) companies (i.e. limited liability companies and stock companies) owned by public enterprises, (iii) companies the sole owner of which is the Republic of Serbia, autonomous province, local self-government unit, as well as subsidiaries the sole owner of which are the respective companies, and (iv) other companies and entrepreneurs to which competent authorities entrusted the performance of these activities ("Specific Entities").

Although the Law on Energy generally prescribes that energy related activities can be performed by public enterprises and by companies and other legal entities or entrepreneurs which have licenses for performing the respective activities, the energy related activities which are identified by the Energy Law as the activities of general interest (thus, the electricity and natural gas related activities identified as such as well) can be performed only by the Specific Entities.

This question is relevant from the perspective of cloud usage as well. The reasoning behind this are the rules envisaged by the Electronic Governance Law[115]. Under this law, all state authorities and organizations, as well as authorities and organizations of autonomous province and local self-governance units, institutions, public enterprises and special authorities through which regulatory activities are performed, but also all legal entities and natural persons entrusted with public authorizations ("**Restricted Entities**"), are obliged to keep all their electronic registries and records, as well as electronic communication accounts, in the Republic of Serbia[116] ("**Localization Rule**"). Moreover, the law prescribes the existence of so-called State Cloud intended to be used by the Restricted Entities, as well as the State Center for Managing and Storing Data as the infrastructure (physical and virtual) the purpose of which is to keep the computers,

[113] "Official Gazette of the Republic of Serbia", no. 15\2016.
[114] Public enterprises are companies which perform activities of general interest and which are founded by the state (i.e. by the Republic of Serbia, autonomous province or local self-government unit).
[115] "Official Gazette of the Republic of Serbia", no. 27/2018.
[116] Exceptionally, the electronic communication accounts of the authorities which perform their activities out of Serbia can be located abroad, under condition that the prescribed security measures are undertaken.

servers, network and security systems necessary for the electronic administration's functioning.

Therefore, the use of cloud located out of Serbia is not allowed for any of the Restricted Entities irrespective of the field or industry they belong, for the purposes of electronic registries and records, as well as electronic communication accounts. The Localization Rule is equally applicable to the Restricted Entities in the field of energy as well (including, amongst other, electricity and natural gas related activities). On the other hand, when it comes to other entities which may be engaged in energy-related activities, i.e. those which should not be regarded as Restricted Entities (such as fully privately-owned business subjects not entrusted with any public authorizations), the Localization Rule is not applicable to them. There are no other restrictions for such entities to use cloud services either locally or abroad.

1.2 Mining

The Law on Mining and Geological Explorations[117] is the principal law governing mining and mineral and other geological resources. With regard to coal related activities, the Energy Law is relevant as well since coal is explicitly prescribed by the respective law as one of energy-generating products.

Given that geological resources are natural assets owned by the Republic of Serbia and that some of them (including coal) are mineral resources of strategic importance, the respective resources' related activities are subject to numerous regulatory requirements. However, we will concentrate on potential information systems regulations.
With regard to the information system in the field of geological explorations and mining, it is envisaged by the law that the competent ministry keeps numerous information systems and cadastres, including, amongst other, the Geological Information System of Serbia and Information System for Geological Explorations and Mining. These two information systems are an integral part of the unified information system of the Republic of Serbia and data contained in these two information systems are public or available for use in accordance with the law.

The law prescribes multiple regulatory requirements on mining and geological explorations' related activities, but we have not identified any restrictions for cloud usage in this field.

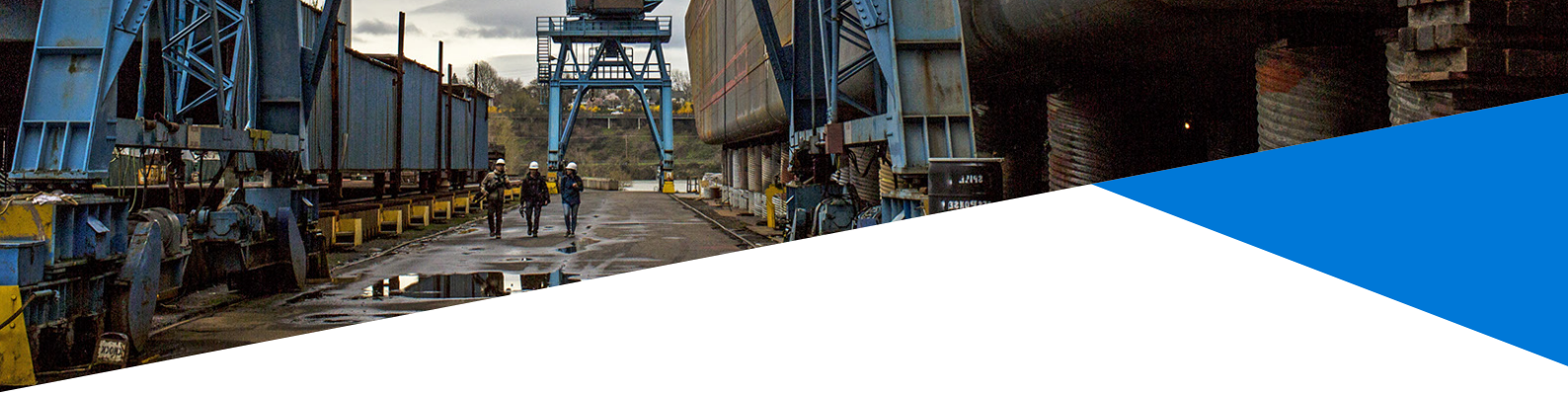
Notwithstanding the above, the Localization Rule, as envisaged by the Electronic Governance Law and as defined herein, is equally applicable to the entities which have competences and/or which perform activities in the field of mining and geological explorations if such entities are the Restricted Entities (such as, for example, state authorities in the respective field).

1.3 Water supply

In the field of water supply and other water related activities, water land and water facilities, the principal law is the Water Law[118]. It contains rules relating to both surface and underground water at the territory of Serbia, including thermal and mineral water, as well as to river sediments which do not include traces of other useful mineral raw materials, with the exception of underground water from which useful raw materials and geothermal energy can be obtained.

The law further envisages detailed rules on water related documentation. This documentation

[117] "Official Gazette of the Republic of Serbia", nos. 101/2015 and 95/2018.
[118] "Official Gazette of the Republic of Serbia", nos. 30/2010, 93/2012, 101/2016 and 95/2018.
[119] Rulebook on Content and Manner of Administering the Water Information System, Methodology, Structure, Categories and Levels of Collecting Data, and on the Content of Data on Which the Public is Notified ("Official Gazette of the Republic of Serbia", no. 54/2011).



includes so-called water book (i.e. registry of issued water documents, such as for example water permits) and several water registries (e.g., registry of water usage, registry of pollutants, and other) which represent a part of the water information system and which are kept by public enterprises (i.e. public water management enterprises). It is explicitly prescribed[119] that data which is kept within this information system is collected, amongst other, by/from business subjects the activities of which influence a water regime. In addition, the Environment Protection Agency keeps the national information system of environment protection which, amongst other, covers water as well.

We have not identified any restrictions for cloud usage in the field of water supply and generally water related activities either, other than the Localization Rule, as envisaged by the Electronic Governance Law and as equally applicable to the entities which have competences and/or which perform activities in the field of water related activities if such entities are the Restricted Entities (such as, for example, state authorities in the respective field).

2. Conclusion

Based on all the above, it can be concluded that the legislation governing all the above activities, i.e. energy (including electricity and natural gas), mining (including coal and precious metals) and geological explorations, as well as water supply and other water related activities, does not impose any restrictions for cloud usage which would be applicable to all the entities performing their activities in the field of the respective industries generally.

The only rule which does impose the cloud usage's restriction for certain type of entities (i.e. for the Restricted Entities, as identified herein) regardless of the field in which they perform their activities is the Localisation Rule imposed by the Electronic Governance Law.

The first step to check whether the Localisation Rule is applicable to a particular entity is to establish whether it can be regarded as any of the Restricted Entities. If so, none of the documentation, i.e. registries or records kept by such entity can be kept in any cloud out of Serbia. If not, the Localisation Rule would not be applicable, i.e. prohibition to "export" data to a cloud out of the country would not exist as such.

Nevertheless, even in the case when the respective prohibition does not apply, the other restrictions and/or specific regulatory requirements may be applicable depending on the type of the respective data (e.g., with respect to personal data under the Serbian Data Protection Law[120]) and related statutory obligations (such as obligations of confidentiality and/or secrecy and/or technical/technological requirements envisaged as obligatory for the entities performing their activities in the above-described industries).

[120]For the sake of completeness, it should be mentioned that Serbia currently has two Data Protection Laws – one is the "old" law originating from 2008 which is applicable until 21 August 2019 and the other is the new law which was adopted and entered into force on 21 November 2018, but with postponed appliance, i.e. appliance as of 21 August 2019.

[121]"Official Gazette of the Republic of Serbia", nos. 6/2016 and 94/2017.

In this regard, the Information Security Law[121] should also be taken into consideration. In brief, this is the law which establishes principles and measures for ensuring security of information-communication systems ("**IT Systems**") used by state authorities and other legal entities for performing their activities ("**Systems Operators**").

Under this law, certain IT Systems are regarded as so-called IT Systems of particular importance and their operators are obliged to ensure that particular technical and organizational security measures are undertaken, as well as to adopt internal acts on their IT Systems' security. This also means that, even if they entrust the activities relating to their IT Systems to third persons (including, amongst other, activity of storing data which belongs to the Systems Operators and which relates to their business activities), they are obliged to ensure that adequate security measures are duly undertaken. The reason why we are mentioning this is the fact that, amongst other, the IT Systems used in performing activities of general interest are regarded as the IT Systems of particular importance if such activities are performed, amongst other, in the following fields: (i) production, transmission and distribution of electricity, (ii) production and processing of coal, (iii) exploration, production, processing, transport and distribution of natural gas, and (iv) using, managing, protection and development of goods of general interest (including, amongst other, mineral resources and water).

In any case, none of such other restrictions/requirements (other than the Localisation Rule) should be regarded as a prohibition for the use of cloud. Nevertheless, they may influence the manner and/or scope in which cloud services may be used and/or the choice of such services' providers and this is why they should be taken into consideration.