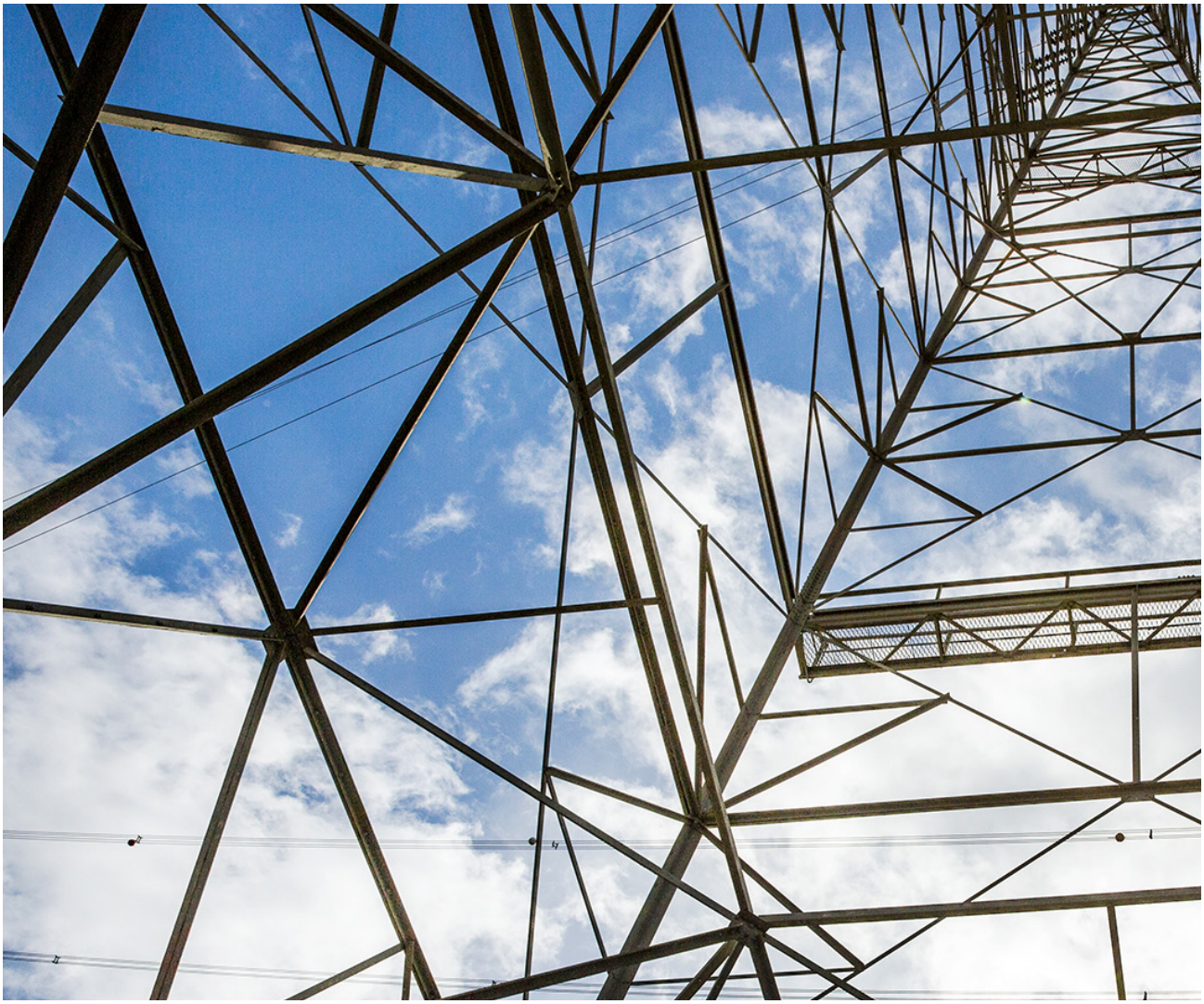
THE LEGAL AND REGULATORY LANDSCAPE FOR POWER & UTILITIES AND OIL & GAS IN KAZAKHSTAN AND UKRAINE



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.

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 challenges 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 both to connect flexible assets, predict and simulate bottlenecks in the grid and through artificial intelligence, enable a 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 ever more important than ever for you to leverage new technologies.

Microsoft helps Power & Utilities companies to become 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.

Digital Transformation of the Oil & Gas Industry

In the Oil and Gas Industry, the adoption of digital tools is increasing, but it's fair to say that adoption is still limited to the use of basic digital tools.

In a recent survey, only 48% of refiners rated themselves as mature or semi-mature in digital technology deployment compared to 44 percent in 2017[1]. The same survey noted that 75 percent of refiners "stated that they intend to spend more on digital over the next three to five years."

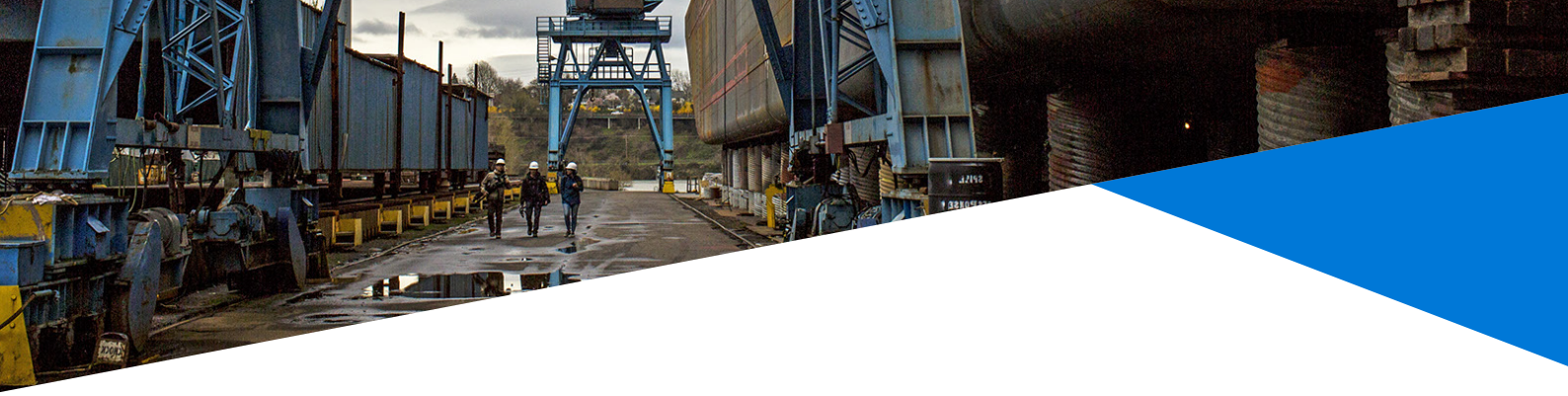
Most companies are still using basic cloud computing or APC (advanced process control) and 80% of Oil & Gas companies realize limited value from digital[2]. The main focus for digital transformation is in the traditional areas like maintenance and reliability with process safety, production planning & scheduling, and production execution. There is limited value derived from digital technology in other key areas like health and safety, energy management, engineering, quality, trading and hydrocarbon supply chain.

Most oil and gas companies have not transitioned to artificial intelligence, block chain and robotics.

Nevertheless most executives agree that the limited investment in digital transformation exposes them to key risks: loss of competitive advantage, inability to reduce costs, limited ability to increase plant reliability and the limited ability to reach to market dynamics. Increasingly O&G companies identified the lack of workforce digital skills as a major barrier to deploying digital technologies in the sector.

New technologies in the last 5 years

Meanwhile it is a 'public secret' that most players in Oil & Gas sit on reservoirs of data, collected and captured over decades, that is only being leveraged to a minimum extend. The major reason for this is lack of methodologies and technologies that allow transforming, often meaningless data, into valuable insight and added value. Primary enablers for this are the ever-decreasing cost of storage and increasing processing power. This, with the cloud becoming the de-facto platform for storing, correlating and processing data amongst value chains, opens a new window of opportunity.



A window of opportunity that triggered a long list of innovations including:

- Mixed reality, combining real world and augmented scenarios. Augmented scenarios that are data driven and created in a digital and often virtual world. Allowing us to project, simulate and test specific changes in the real world. Helping us making better considerations and changes. Examples are construction of new plants or assets, simulating and evaluating specific HSE scenarios, and training key staff.
- Cloud computing becomes the preferred platform because of scalability, accessibility, connectivity, manageability and even security.
- Edge-computing, combined with an increasing variety of innovative smart sensors, allows us to monitor, control and predict behaviour and performance of nearly every key component across processes.
- Artificial intelligence, allowing prediction of probable scenarios or anomalies based on correlating real time / near time data with historical data.
- BOT-services, allowing humans to easily interact with data through natural language.
- Computer vision, recognizing real time visuals and recognizing, matching and interpreting them against predefined rules and scenarios.

Data (both historical and actual) are feeding all innovative technologies above and help us to better understand and control processes, aiming at higher levels of excellence, safety and efficiency.

[1]https://www.accenture.com/_acnmedia/pdf-79/accenture-2018-refining-research.pdf
[2]https://www.accenture.com/us-en/insights/industry-x-0/2018-digital-refining-survey

The legal and regulatory landscape

This Whitepaper analyses 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, as well as for the Oil & Gas sectors, in Kazakhstan and Ukraine.

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

- KAZAKHSTAN: Shakhrukh Usmanov (Partner), GRATA INTERNATIONAL
- UKRAINE: Iryna Kalyta (Associate Partner, Attorney-at-Law), EY UKRAINE

Kazakhstan

Legal research into the use of cloud services for critical infrastructure in Kazakhstan April 2019

1. Overview

In Kazakhstan the regulation of cloud services and critical infrastructures is carried out predominantly by the information security bodies and, in a lesser extent, by other industry-specific authorities. Key regulatory bodies which regulate cloud services and critical infrastructures will be outlined in the relevant section of this research.

Cloud services in Kazakhstan are generally regulated by a number of legislative acts, which are practically silent on the legal definition of *cloud* or *cloud services*. The legal framework does not expressly define general terms of use nor does it establish special requirements for the use of cloud services, to the extent established in other areas of information technology law.

Industry sectors including power, utilities and oil & gas do not establish firm and clear requirements for implementation of cloud technologies into these industries either. Basic requirements provided in the industry-specific legislation refer to regulatory barriers that are mainly related to confidentiality of data.

2. Analysis

2.1 Notion and use of cloud services and critical infrastructures in Kazakhstan

Cloud Services: Generally, Kazakhstan laws do not provide for a definition of *cloud or cloud services* notwithstanding some pieces of legislation actually regulate the use of cloud services in Kazakhstan. One of those pieces is the Informatisation Act[3] which in principle regulates[4] the area of informatisation within the territory of the Republic of Kazakhstan and the relationship between government bodies, individuals and legal entities for creation, development and operation of informatisation assets.

[3]Act of the Republic of Kazakhstan of 24 November 2015 No. 418-V "On Informatisation"
[4]Preamble to the Informatisation Act

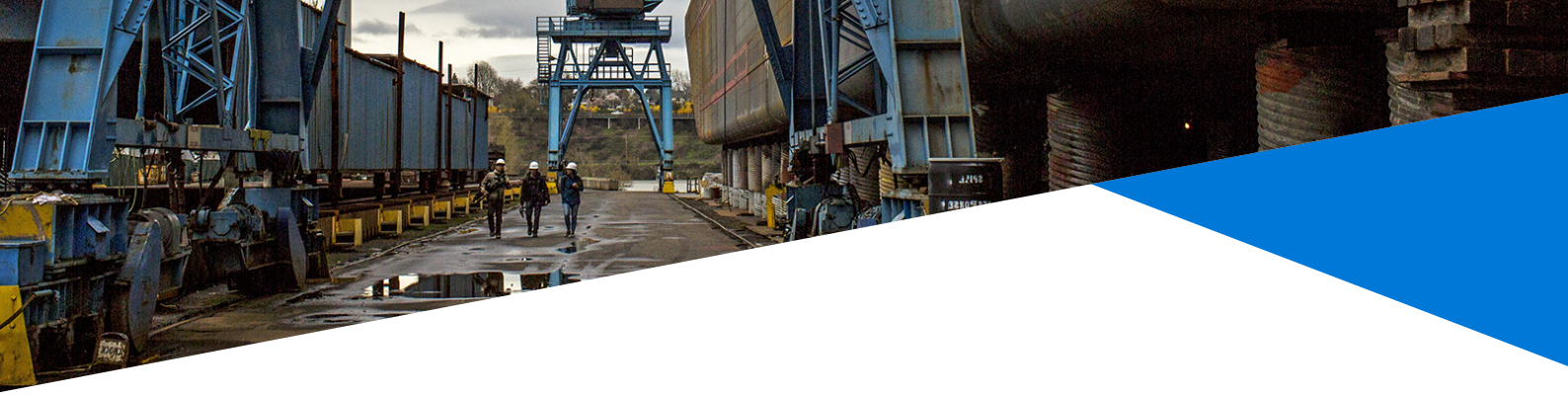
The term *informatisation asset*[5] is key not only for understanding how the Informatisation Act works but also how cloud services could relate thereto. Basically, the term covers electronic information resources, software, internet resources [e.g. websites], and information and communication infrastructure. Each of the aforesaid categories has its own classification[6] and subcategories under the Informatisation Assets Classification Rules e.g. one of the subcategories of software relates to system-wide software[7] which is designated for ensuring effective management of hardware resources related to technical devices, development and functioning of applied software, software service products, information systems and internet resources. The system-wide software also covers cloud and virtualisation management software (CVMS)[8] and cloud infrastructure management software (CIMS)[9]. Thus, from the perspective of informatisation assets categories, cloud services are classified as system-wide software in particular, and as informatisation asset in general.

Critical Infrastructures: Another aspect of the use of cloud services within the territory of Kazakhstan is the functioning of assets within the information and communication infrastructure, which may be of critical importance or *critical infrastructure assets*[10]. Generally, assets of information and communication infrastructure (including critical infrastructure assets) encompass[11] information systems, technological platforms, hardware complexes, server facilities (data processing centres), telecommunication networks, as well as information security systems and uninterruptable functioning of technical devices systems. It is, therefore, suggested that the range of assets of information and communication infrastructure is quite broad. The assets fall within the category of critical infrastructure assets in the event the breach or termination of the asset's functioning lead to emergency of social and (or) man-triggered character or significant negative implications for the defence, security, international relations, economy, particular industries, infrastructure of the Republic of Kazakhstan or for the public life-sustaining activity within the territory. The government bodies of the Republic of Kazakhstan specify criteria for identifying critical infrastructure assets and approve the list of critical infrastructure assets functioning in the industry-specific areas which will be considered herein below.

2.2 General provisions on industry specific sectors

It should be noted that the majority of the industry-specific sectors, such as power, utilities and oil & gas, reviewed in this research paper are subject to regulation in the area of natural monopolies. In particular, the Natural Monopolies Act applies to such sectors[12] as trunk pipeline oil and gas transportation and storage, transmission of electric power, sewage and water supply. Under the Natural Monopolies Act the government regulation of natural monopoly subjects and their activity is carried out according to the principle of availability for the public i.e. *'information shall not be regarded as trade (commercial) secret if the information is provided by the natural monopoly subject for the purpose of tariffs approval'* that basically makes the use of privately protected cloud data not as protected as it could be.

[5]Paragraph 4 of Article 1 of the Informatisation Act
[6]Rules on Classification of Informatisation Assets and Classification System of Information Assets approved by the Order of the acting Minister of Investments and Development of the Republic of Kazakhstan of 28 January 2016 No. 135
[7]Subparagraph 6 of Paragraph 3 of Schedule 1 to the Informatisation Assets Classification Rules
[8]Paragraph 3.2 of Annex 1 to Schedule 1 to the Informatisation Assets Classification Rules
[9]Paragraph 3.2.1 of Annex 1 to Schedule 1 to the Informatisation Assets Classification Rules
[10]Paragraph 24 of Article 1 of the Informatisation Act
[11]Paragraph 25 of Article 1 of the Informatisation Act
[12]Paragraph 1 of Article 5 of the Natural Monopolies Act
[13]Paragraph 7 of Article 25 of the Natural Monopolies Act



2.3 Regulation of the power sector

Electricity, Coal and Precious Metals: The power sector of the Republic of Kazakhstan is mainly regulated by the Electric Power Act and Renewable Energy Sources Act. The aforesaid legislation does not explicitly contain industry-specific restrictions related to the use of cloud technologies while carrying out activity within the power sector.

Pursuant to the provisions[14] of the Electric Power Act *'the users of electric power production and transmission have the right to receive technical information necessary for carrying out activity related to production and transmission of the electric power from the system operator'* which is the national company controlling the operation of electricity grid. The system operator carries out a number of functions including the function[15] for *'providing the users of electric power wholesale market with the information which does not concern a trade (commercial) secret or information which is otherwise protected by law'* that may be regarded as condition for the wide use of public cloud services by a particular user within the industry.

In relation to the precious metals used for the production and operation of solar energy components the Renewable Energy Sources Act and other relevant legislative acts of Kazakhstan do not envisage any impediments related to the use of cloud technology for the renewables sector.

2.4 Regulation of the utilities sector

Natural Gas and Water Supply: The utilities sector of the Republic of Kazakhstan is mainly regulated by the Gas Act and Water Code. There are no expressly specified provisions in the aforesaid pieces of legislation that would set up barriers for the free use of cloud technologies in the utilities.

2.5 Regulation of the oil & gas sector

Hydrocarbons: In Kazakhstan the hydrocarbons sector is one of the most developed segment of the country's economy resulting in emerging development of processes both from the law and information technology perspectives. Not long ago (in the end of 2017) the legislation related to hydrocarbons had been significantly upgraded: the act on subsoil and subsoil use was extended and codified into the Subsoil Use Code. Information storage, record-keeping and data registry processes were undergone some modifications and improvements.

The upgrade of subsoil use related legislation, however, has not resulted in introduction of requirements for using specific information and communication infrastructure or regulatory hindrance regarding the use of cloud technologies. For hydrocarbons sector presumes a massive loads of specific technical information which can be open and restricted to public the confidentiality issues and data protection requirements, therefore, may arise in this respect.

In relation to availability and exchange of legal and technical information, free access to information on licences and contracts for subsoil use is provided by the government body[16] except for particular information that constitutes confidential[17] information. The exception relates to the geological information contained in the geological (exploration) reports and other documentation received by the government bodies which shall undertake reasonable measures for keeping the information confidential . The confidential information can be made public in the event of: (a) expiry of five consecutive years as from the day the information has been received from the subsoil user (b) expiry of the contract for subsoil use (c) subsoil user's consent made in writing

[14]Subparagraph 2 of Paragraph 1 of Article 12 of the Electric Power Act
[15]Subparagraph 12 of Paragraph 1 of Article 10 of the Electric Power Act
[16]Paragraph 1 of Article 77 of the Subsoil Use Code
[17]Paragraph 3 of Article 77 of the Subsoil Use Code

(d) request made by other government bodies subject to undertaking measures for protection of confidentiality of the information obtained (e) other circumstances specified by the Subsoil Use Code.

In relation to private use of the cloud opportunities in the hydrocarbons sector no significant barriers related to corporate cloud technologies can be found in Kazakhstan laws whereas the government related sector that, in turn, requires some involvement of information technologies (e.g. public procurement) would probably be reluctant to introducing the cloud into operation for some time.

2.6 Cloud services and personal data protection

Personal Data Protection Requirements: In respect of personal data protection Kazakhstan laws provide for two key requirements: (a) localisation requirement and (b) cross-border transfer requirement.

Pursuant to the provisions[18] expressly stated in the Personal Data Protection Act *'storage of personal data shall be carried out by the data controller and (or) data processor, as well as a third party, in the database which is located within the territory of the Republic of Kazakhstan'*. At the same time Kazakhstan laws do not prohibit simultaneous (so called, parallel) storage of personal data both within and outside the territory of Kazakhstan. Another requirement relates to cross-border transferring of personal data that basically requires[19] *'consent of the data subject to cross-border transfer of data subject's personal data' unless the country, where the personal data* is transferred to, ensures[20] protection of personal data (i.e. countries which are parties to the Strasbourg Convention).

Apparently, these two statutory requirements related to personal data localisation and cross-border movement of personal data may apply to cloud usage in Kazakhstan thus imposing conditions for the use of foreign cloud services by local users.

3. Conclusions

Kazakhstan laws do not specify the definition of cloud or cloud services in the public general acts of Kazakhstan (save to particular classification provided in the by-laws) although cloud services are used and regulated within Kazakhstan.

Kazakhstan laws applicable to industry specific sectors (i.e. power, utilities and oil & gas reviewed in this research) do not expressly impose restrictions on the use of cloud services that may prevent cloud services by the industries from the unrestricted use within the territory of Kazakhstan.

Kazakhstan laws in the area of personal data protection set out certain conditions for cloud service providers for rendering cloud services in Kazakhstan in cases where such services are provided with use of data bases located outside Kazakhstan. Kazakhstan legislation has a direct requirement on storing personal data of citizens of Kazakhstan in the territory of Kazakhstan, however, Kazakhstan law allows under certain conditions cross-border transfer of personal data and does not prohibit parallel storage of personal data inside and outside Kazakhstan, therefore, the localization requirement should not be perceived as a direct prohibition or blocker for usage of foreign cloud solutions as such. This approach is supported by the practice of the Kazakhstan government authorities, however, this approach has not yet been formalized and is subject to clarification.

[18]Paragraph 2 of Article 12 of the Personal Data Protection Act
[19]Subparagraph 1 of Paragraph 3 of Article 16 of the Personal Data Protection Act
[20]Paragraph 2 of Article 16 of the Personal Data Protection Act

Ukraine

1. Overview

Below we outline the general Ukrainian legal requirements for the use of cloud solutions in critical infrastructure in the following sectors: **Power** (electricity, coal and precious metals), **Utilities** (natural gas and water supply), and **Oil and Gas.**

Information technology environment of Ukraine is constantly evolving. An accelerated shift from traditional on-premises IT systems to cloud technologies is inherent to this process. Ukraine recognizes the importance of shifting towards the cloud and this is reflected in a number of Ukraine domestic policies. For example, the Cabinet of Ministers of Ukraine adopted several national strategies that stress the need to utilize the cloud, IoT and other modern technologies.[21]

Ukrainian law defines cloud computing system as a system that embodies a model of a demand-driven access to a common set of dynamically distributed customizable computing resources (including intranets, servers, data storage, applications, and services) that can be promptly provided and released through global data networks with minimum managerial efforts and/or minimal interaction with a cloud service provider.

However, Ukraine has no regulations explicitly governing the use of cloud solutions.
In 2016, the Ukrainian parliament considered Bill No. 4302 that was supposed to introduce a number of general rules for using cloud computing in public sector. This bill was approved in the first reading. In February 2019, this bill was listed for the Parliament's latest legislative session, but it has not been voted yet.
In the absence of special rules the usage of cloud computing systems within critical infrastructure is governed by general Ukrainian cybersecurity, information protection and personal data protection rules and restrictions. This legal framework contains a number of gaps and uncertainties.

[21]Reference is made to Order of the Cabinet of Ministers of Ukraine 'On Approval of the E-government Concept in Ukraine' No. 649-p dated 20 September 2017 and Order of the Cabinet of Ministers of Ukraine 'On Approval of the Concept of Development of Digital Economy and Society in Ukraine for the Years 2018 – 2020 and Approval of the Plan of Measures for its Implementation' No. 67-p dated 17 January 2018.

2. What is critical infrastructure

Ukrainian regulations dealing with critical infrastructure ('**CI**') are still being developed. The definition of critical infrastructure could be found in law of Ukraine 'On Main Principles of Maintaining Cybersecurity of Ukraine' (the '**Law on Cybersecurity**'), which came into effect in 2018.

The Law on Cybersecurity defines CI object as a public or private legal entity the activities of which relate to technological processes and/or provision of services that are critical for the economy, the industry, the functioning of society and public security. Damage to such entities could negatively impact state security, defense, environment and could cause considerable financial losses and/or be a threat to life and health of people.

A legal entity could be classified as a CI object if it:

- carries out works and provides services in energy, chemical, transport, information and communication technologies, electronic communications, banking and financial sectors; and/or
- renders services for public life support, in particular in areas of centralized water supply, drainage, supply of electrical energy and gas, food production, agriculture and health care; and/or
- belongs to a municipal, emergency and rescue service; and/or
- is on the list of strategically important enterprises to the state`s economy and security; and/or
- is on the list of objects of potentially dangerous technologies and industries.[22]

The lists of strategically important enterprises and objects of potentially dangerous technologies and industries are available to public.[23] However, the fact that a legal entity is on this list does not mean that it automatically obtains status of a CI object.

Communication and technological system of a CI object, which, if attacked, will impact the operations of the CI object, is considered to be an object of critical information infrastructure. The Cabinet of Ministers of Ukraine (the 'CMU') should adopt the list of CI objects and the list of objects of critical information infrastructure. There is a 2016 CMU regulation laying down the procedure for determining the list of critical information infrastructure, but it has not been aligned with the Law on Cybersecurity yet.[24] The list of critical information infrastructure approved under this regulation is classified and is not publicly available. New relevant CMU regulations are still in drafts as of June 2019.

So, there is no full clarity regarding the list of entities qualifying as CI, and the list of critical information infrastructure which is subject to cybersecurity requirements.

Classification of an entity as a CI is not automatic; not all oil and gas, power and utility sector companies will be considered CI. The entities which are not on the list of CI are subject to general, less stringent information protection rules. Both public and private entities could be on CI list.

[22]Article 6 of the Law on Cybersecurity.
[23]Reference is made to Regulations of the Cabinet of Ministers of Ukraine No, 83 dated 4 March 2015 and No. 956 dated 11 July 2002.
[24]Reference is made to Regulation of the CMU 'On Approval of a Procedure of Formation of the List of Information and Telecommunication Systems of Critical Infrastructure Objects of the State' No. 563 dated 23 August 2016.

3. Cybersecurity rules for CI

The Cybersecurity law envisages that objects of critical information infrastructure are subject to cybersecurity measures. The term 'cybersecurity' envisages that the CI systems should be protected by a set of organizational, legal, engineering and technical measures aimed at prevention of cyber-incidents, detection and protection from cyber-attacks, remedying the impact and recovery of communicational and technological systems.

The current secondary regulations state that protection of IT systems of the state CI from cyber-attacks is ensured by the system owner (processor) in accordance with regulations on cybersecurity and protection of information[25].

So, there is a general requirement that both public sector and privately-owned CI should be subject to cybersecurity rules.

In the absence of specific laws and regulations on cloud in Ukraine information protection rules for critical infrastructure will apply to CI entities from Utilities, Oil and Gas and/or Power sectors.

The CMU has adopted CI-specific General cybersecurity rules that introduced more stringent requirements of information protection for critical information infrastructure as compared to the general information protection rules. Cybersecurity of CI object should envisage implementation of a comprehensive information protection system or information security system with verified conformity.[27]

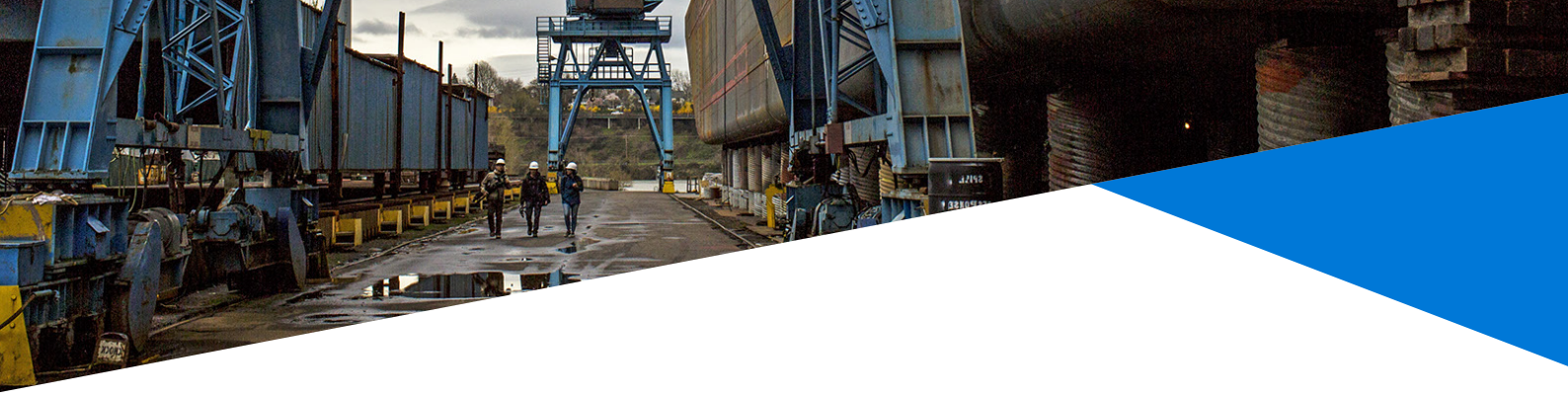
General rules contain extensive cybersecurity requirements for CI. To name a few:

- Components and/or information of the object of critical information infrastructure of a CI could be held in a third-party datacenter only provided that: (i) such datacenter is located in the territory of Ukraine, and (ii) the datacenter is owned by a Ukrainian resident. Agreement with the datacenter should stipulate its commitments to comply with the relevant cybersecurity special rules.
- Components and/or information of the technological processes control system of CI object could be held only in its own datacenter.
- The technological process management system could be connected global networks, including Internet, only if technological process cannot function without Internet.

However, the CMU rules contain a general exception saying that if any of the General requirements cannot be implemented, or if there is no possibility to implement it without negative impact on CI functionality, or due to specifics of CI, then it is possible not to apply the requirement but to implement compensating measures instead and document the exception[28].

Considering that CI cybersecurity rules have been adopted very recently, legal framework covering information protection within CI contains a lot of uncertainties. In addition to the general CI cybersecurity rules, Ministries and other executive authorities are allowed to develop more detailed CI cybersecurity requirements for specific sectors that they control, so regulatory framework is still developing.

[25]Item 5 of Regulation of the CMU 'On Approval of a Procedure of Formation of the List of Information and Telecommunication Systems of Critical Infrastructure Objects of the State' No. 563 dated 23 August 2016.
[26]Reference is made to Regulation of the CMU 'On General Requirements to Cybersecurity of Objects of Critical Infrastructure' No. 518 of 19 June 2019, which took effect at the end of June 2019.
[27]Item 3 of the General requirements, approved by Regulation of the CMU 'On General Requirements to Cybersecurity of Objects of Critical Infrastructure'.
[28]Item 13 of the General requirements, approved by Regulation of the CMU 'On General Requirements to Cybersecurity of Objects of Critical Infrastructure'.



Only those sector entities listed as CI objects by the CMU will be subject to special cybersecurity rules. Other oil and gas, power and utility sector entities will remain subject to general information protection rules, which depend on whether the entity belongs to the public sector and on the types of information it processes.

The general rules are more stringent for the state-controlled entities. So, a privately owned and a state-controlled entity from oil and gas, power or utility sector could be subject to different information protection rules.

4. Different types of information and their legislative framework on protection of information

Information protection regime in Ukraine is governed by a number of laws and regulations.[29] In addition an extensive network of secondary legislation and technical regulations deal with specific aspects related to protection of information. Special rules and restrictions apply to entities providing state electronic services. Ukraine information protection requirements primarily depend on (i) type of information and (ii) whether it is related to public sector.

Ukrainian law generally divides information into two major groups: **open** and **classified**[30]. There are also special rules applying to **personal data.**

All information is regarded as open, unless it is classified by law[31]. Open information may circulate freely provided it does not qualify as 'state information resources' or relate to activities of public bodies, military formations, which is disseminated in the Internet, other global information networks and systems or transferred through telecommunication networks.

Classified information includes: confidential information, official information, secret information (including state secrets and other secret information). State secrets are awarded the strictest information protection regime.

The majority of open information can be moved to cloud freely without any additional restrictions, while moving classified data into cloud will require case by case assessment. However, for state information resources and personal data special requirements apply.

4.1 General requirements for information protection for state information resources and classified information

Ukrainian laws and regulations on security of

[29]inter alia:
a) Law of Ukraine 'On Information'
b) Law of Ukraine 'On Information Protection in Information and Telecommunication Systems'
c) Law of Ukraine 'On Personal Data Protection'
d) Law of Ukraine 'On Access to Public Information'
e) Law of Ukraine 'On State Secrets'
f) Law of Ukraine 'On Cybersecurity'
g) Regulation of the Cabinet of Ministers of Ukraine 'On the Rules on Provision of Information Protection in Information and Telecommunication Systems'
h) Decree of the President of Ukraine 'Regulation on Procedure of Conducting Cryptographic Protection of Information in Ukraine'

[30]Article 20 of law of Ukraine 'On Information' No. 2657-XII dated 2 October 1992.

[31]Paragraph 2 Article 20 of law of Ukraine 'On Information' No. 2657-XII dated 2 October 1992.

information require that state information resources and classified information subject to protection requirements should be safeguarded by a comprehensive information protection system ('**CIPS**').

The definition of state information resources is wide and includes *'information possessed by state authorities and military formations, state enterprises, institutions and organizations, as well as information creation of which is provided for by the law and which is processed by private individuals and legal entities as permitted by public authority'*.[32] So, all types of information circulating within CI information systems processing state information resources or other classified information protected by law require protection by the comprehensive information protection system.

Thus, public sector entities in oil and gas, power and utilities will have to comply with CIPS rules, regardless of whether they are on the list of CI. Privately-owned legal entities will only be subject to these rules if they possess classified information protected by law.

CIPS is defined as a combination of organizational, engineering and technical measures, means and methods of information protection.[33] There are two key requirements with respect to application of CIPS:

- **Certification/examination of components.** The CIPS may only be established using means of information protection that have conformity certificates or positive expert opinions based on the results of state examinations in area of technical protection of information (the '**TPI**') and/or cryptographic protection of information (the '**CPI**')[34].

- **Application of CIPS; state examination.** The law mandates that state information resources or classified information subject to protection in accordance with the law must be processed in information systems using CIPS with verified conformity. The conformity of CIPS is verified by a state examination procedure.[35]

These procedures are complex, and they have not been adapted for the systems using cloud products. They contain a number of regulatory or technological requirements or restrictions that may limit the possibility of using cloud solutions.

4.2 Industry-specific rules on data management

CI in Power, Utilities and Oil and Gas sector are often state-owned and are likely to manage either state information resources or classified information of different types due to the nature of their activities. Below we provide a few examples.

4.2.1 Power (electricity, coal and precious metals)

Electricity. Market operators from the electricity sector (transmission system operators, distribution system operators and an operator of electricity market) are obliged to protect confidentiality of information received from electricity market participants, *inter alia,* producers[36]. Information regarding trading on day-ahead and intra-day electricity markets is state property. This triggers

[32]Subparagraph 6 of Paragraph 1 of Article 1 of law of Ukraine 'On the State Service of Special Communication and Information Protection of Ukraine' No. 3475-IV dated 23 February 2006.
[33]Article 1 of law of Ukraine 'On Information Protection in Information and Telecommunication Systems' No. 80/94-BP dated 5 July 1994.
[34]Paragraph 3 of Article 8 of law of Ukraine 'On Information Protection in Information and Telecommunication Systems' No. 80/94-BP dated 5 July 1994.
[35]Paragraph 2 of Article 8 of law of Ukraine 'On Information Protection in Information and Telecommunication Systems' No. 80/94-BP dated 5 July 1994.
[36]Articles 33, 46, 51 of law of Ukraine 'On Electricity Market' No. 2019-VIII dated 13 April 2017.
[37]Sections 6, 7 of Regulation of the National Commission for State Regulation of Energy and Public Utilities 'On Approval of the Rules of a Day-ahead and Intra-day Markets' No. 308 dated 14 March 2018.

specific requirements on information protection.[37] There is a 'presumption of confidentiality' applicable on the electricity market, where regulations set an exhaustive list of information subject to publishing by the operator of electricity market in Ukraine.

Precious metals. Information on official reserves of monetary precious metals and precious gems is considered to be state secret.[38] Information on coal, oil and gas mineral deposits is subject to general information protection rules.

4.2.2 Utilities (natural gas and water supply)

Utilities sector follows general information protection rules. However, there is a specific requirement that information on the quality of water should be open to the public.[39]

4.2.3 Oil and Gas

Ukrainian law provides for specific rules regarding the use of geological information.[40]

The geological information covers geological structure of the mineral resources, mineral deposits, the composition of raw materials and properties of rocks, ores, minerals, hydrocarbons, groundwater, as well as other qualitative and quantitative parameters, indicators and features of mineral resources.

The rights to geological information may be transferred on the contractual basis. However, should the possession of the state-owned geological information be delivered to another user on the contractual basis, it is prohibited to transfer it further.

Certain categories of geological information is considered to be state secrets. For example, information regarding[41]:

- capacity of oil (gas) underground storage in Ukraine;
- perspectives of exploration or extraction of minerals in Ukraine, the disclosure of which may harm public security (the decision on secrecy is taken by a state expert on secrets);
- specific indices on the systems of external supply lines of electric and thermal energy, gas pipelines intended for feeding enterprises, institutions, organizations producing arms;
- precious metals (as mentioned above).

In addition, Ukrainian regulations outline that a wholesale supplier of natural gas market should retain information regarding all transactions with wholesale buyers and other suppliers for a five years period and make it accessible to the competent authorities.[42] This information may be subsequently disclosed, unless it jeopardizes commercial interests of market participants.

[38]Subparagraph 5 paragraph 2 Article 8 of law of Ukraine 'On State Secrets' No. 3855-XII dated 21 January 1994.
[39]Article 9 of law of Ukraine 'On Drinking Water, Drinking Water Supply and Drainage' No. 2918-III dated 10 January 2002.
[40]Regulation of the Cabinet of Ministers of Ukraine 'Regarding the Disposal of Geological Information' No. 939 dated 7 November 2018; Article 33 of law of Ukraine 'On Oil and Gas' No. 2665-III dated 12 July 2001.
[41]Order of the Security Service of Ukraine 'On Approval of the List of Information that is Assigned to State Secret' No. 440 dated 12 August 2005.
[42]Article 17 of law of Ukraine 'On the Natural Gas Market' No. 329-VIII dated 9 April 2015.

5. Technological requirements applicable to CI

The legal provisions analyzed herein contain no explicit prohibition to use cloud solutions for CI objects.

However, CI cybersecurity rules and national information protection rules contain a number of regulatory or technological restrictions or requirements that may limit the possibility of using many cloud solutions by the public sector in general and also by CI in Power, Utilities and Oil and Gas sectors in Ukraine. Below we highlight some of these requirements:

5.1 Connection to internet

there is an absolute prohibition to connect local networks and separate computers that process or store **state-owned** classified information subject to protection by law to global data transmission networks, including the **Internet**.[43]

For CI, the technological process management systems could only be connected to Internet if technological process cannot function without Internet, and provided that all cybersecurity measures are in place. Components or information of the technological processes control system of CI object could be held in its own datacenter only[44].

5.2 Personal data

under the Law 'On Personal Data Protection' only state or municipal enterprises may act as processors of personal data if state or municipal authorities are its controllers[45]. This provision does not prohibit the use of cloud solutions for processing personal data controlled by state or municipal authorities, but limits the list of potential processors for this type of data by the state or municipal enterprises.

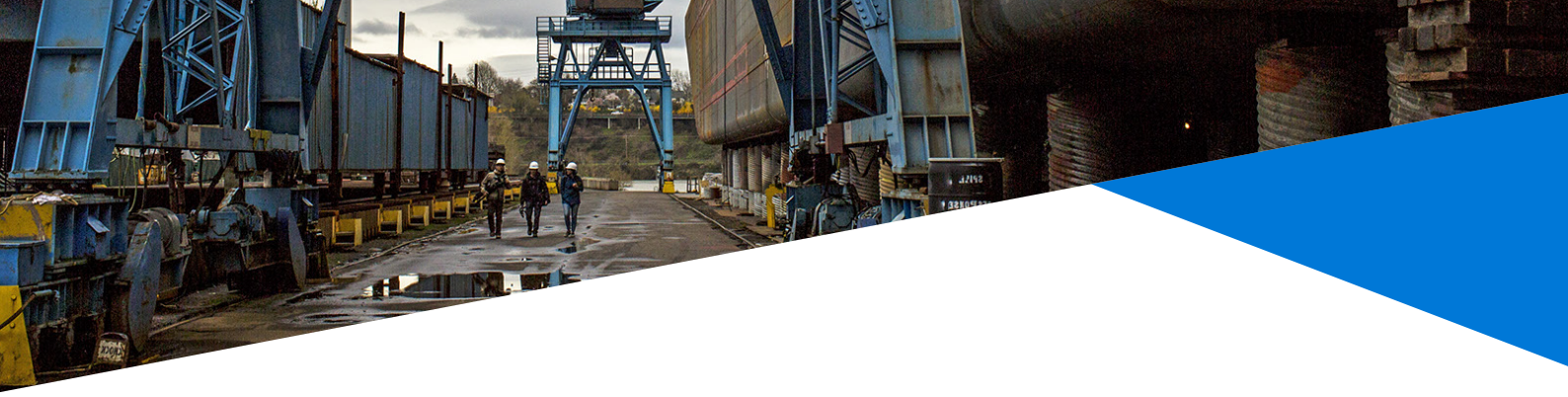
5.3 Two-level conformity confirmation procedure

Ukrainian regulations provide for a two-tier structure for verifying conformity of information protection within computer systems which process state information resources or classified information that should be protected by law.

- First, all of the information system components must be either certified or examined with respect to technical protection of information (TPI) and/or cryptographic protection of information (CPI);
- Second, each specific information system which must be examined as a whole for compliance with requirements to the comprehensive information protection system (CIPS).

These procedures are complicated. The feasibility of cloud solutions successfully passing these procedures are subject to an uncertainty and could depend on

[43]Paragraph 7 of Regulation of the Cabinet of Ministers of Ukraine 'On Approval of the Procedure of Connection to the Global Data Transmission Networks' No. 522 dated 12 April 2002.
[44]Item 36, 49 of General requirements, approved by Regulation of the CMU 'On General Requirements to Cybersecurity of Objects of Critical Infrastructure' No. 518 of 19 June 2019.
[45]Paragraph 3 of Article 4 of law of Ukraine 'On Personal Data Protection' No. 2297-VI dated 1 June 2010.



the cloud product. So, the possibility of using cloud by public sector should be analyzed case by case. Private sector oil and gas, power and utility entities are not currently subject to these rules, except as they are on the CI list or possess classified information protected by law.

5.4 Domain registration

Ukrainian regulation that covers procedure of domain registration for state authorities envisages that state electronic information resources (for the purpose of which a domain name is being registered) should be stored using program / technical means that are located in the territory of Ukraine.

6. CONCLUSIONS

The legal provisions analyzed herein contain no absolute prohibition to use cloud solutions for critical infrastructure in Power, Utilities and Oil and Gas sectors in Ukraine.

However, national information protection rules and CI cybersecurity rules contain a number of regulatory or technological restrictions or requirements that may limit the possibility of using cloud solutions by the public sector in general and CI in Power, Utilities and Oil and Gas sectors in Ukraine. These requirements should be considered when developing IT systems infrastructure based on cloud products.