Overview of the legal framework in Romania and the European Union on Upstream Data handling

31 October 2019

List of acronyms

ANRM	National Agency for Mineral Resources of Romania
EU	European Union
SRI	Romanian Intelligence Service
Upstream Data	digital and hard copy Geodata *e.g*. production, deposits, geological studies, nature reserves and related operational data within the Oil & Gas exploration activity

1. Executive Summary

1.1. Objective of the study

This study aims to present the current status of the legal framework in Romania and at European level, in four jurisdictions selected for this study, *i.e*. Italy, Hungary, Norway and Poland, on the legal regime and the manner in which oil and gas Upstream Data are handled, processed, modified, disclosed, transferred, altered by their owners / users (*i.e*. economic operators, licensees under petroleum concession agreements).

Further, the study presents the main advantages and disadvantages of the legislative approaches identified in the states mentioned above, and aims to identify potential any improvement areas in respect of the Romanian legislation, for the enhancement of the economic activity of the involved parties and support of investors in the upstream sector.

References to previous public studies issued at European level are also made within this document.

1.2. Key findings

- The tendency at European level is in the sense of removal / limitations of restrictions and barriers which exist at this moment in the member states of the EU with regard to the transfer, use, storage, processing and access of the data without personal character.
- Apart from Romania, out of the analysed member states, we have not identified territoriality requirements for data specific to the Upstream industry;
- In all the analysed states, the nature of the Upstream data is confidential, with several states including certain information in the public domain (the classification as „restricted information" (in Romanian, secret de serviciu) (was not identified in any of the states).
- In Romania, for the transfer of data it is necessary to obtain approval of ANRM, while in the majority of states it is sufficient to obtain the consent of the owner of the license. Hungary imposes the approval of the competent authority for the category entailiing data used for justifying a decision issued by the authority.
- There is a consensus at European level that openness towards technology is necessary for the economy of the EU, leading to growth of the productivity, competition and even ensuring the continuance of certain industry fields. In this sense, the Non personal Data Regulation was adopted.
- Some member states within the EU begun to eliminate data localization restrictions (Estonia, Denmark).

1.3. Key steps for improvement

1. Removal of unjustified barriers which take the form of localization data may trigger multiple operational advantages in all areas, including in the oil and gas industry:
    - easing access of the owner of the data and its users
    - increasing of the cooperation between economic operators and authorities
    - optimizing traceability of the persons which take contact with the respective data.
2. At a strategic level, adoption of new technology is the premises for

creation of value, both for the Romanian State, as well as for companies from the oil and gas sector.

3. In the context of the obligation imposed by the European Regulation no. 2018/1807 on the member states ro reanalyze the legislation in view of removal of restrictions it is recommendable to immediately consult the industries impacted by the respective restrictions.

4. The review of the legislative framework would lead to an increase of the interest of the investors in relation to the oil and gas upstream projects, to the creation of a national database to be further used for better-substantiated energy policies, would ease the cooperation between the operators and the national authority. At the same time, the declassification of certain data would simplify the procedures at the level of the Romanian public bodies and may trigger a decrease in the number of the persons involved in the handling of such data.

2. Methodology and input data. Romanian legal framework

2.1. Presentation of methodology deployed

This study aims to present the current status of the legal framework in Romania and at European level, in four jurisdictions selected for this study, *i.e*. Italy, Hungary, Norway and Poland, on the legal regime and the manner in which oil and gas Upstream Data are handled, processed, modified, disclosed, transferred, altered by their owners / users (*i.e*. economic operators, licensees under petroleum concession agreements). Further, the study summarizes the main advantages and disadvantages of the legislative approaches identified in the states mentioned above, and aims to identify potential any improvement areas in respect of the Romanian legislation, for the enhancement of the economic activity of the involved parties and support of investors in the upstream sector.

Likewise, we included the main conclusions issued at European level by several European institutions on the matter of non-personal data handling (in general), in the context of the issuance of the Non-Personal Regulation (as defined in this document).

Unless expressly stated otherwise in the study, our analysis is based on matters of Romanian law in force on the date hereof. The matters expressed in this study as of the date hereof, are statements of opinion based on our understanding and interpretation of the laws currently in force. From our practical experience, many issues may arise in relation to the interpretation given to certain provisions of the legislation due to their often ambiguous wording. The absence of a unitary application of the legislation may sometimes lead to contradictory decisions by the courts of law and authorities. Furthermore, Romania is not a precedent-based legal system and therefore the Romanian courts of law are not bound by previous decisions issued on the same matter by other courts of law.

The overview relating to the other member states' legislations was done pursuant to a limitative questionnaire addressed to the Deloitte Legal member lawfirms from three jurisdictions, *i.e*. Italy, Hungary and Poland. The experts with the Deloitte Legal network were asked to answer the following questions:

1. Please provide us a list of the main legal acts applicable in your jurisdiction regulating the manner in which Upstream Data is classified, kept, processed, transmitted, disclosed, archived by petroleum licensees (i.e. economic operators, beneficiaries of petroleum concession agreements)

2. Please indicate under which legal regime the Upstream Data falls under, e.g. permanent/temporary classified information, state secret, restricted information, public information with limited access etc.

3. Please list briefly which are the main legal consequences derived from the legal regime of the Upstream Data referred to at point 2 above, with highlight on the manner in which they must/can be stored, transmitted (internally or to third parties), disclosed, archived, physically protected.
4. Please indicate whether the Upstream Data must/may be stored by the petroleum licensee in both hardcopy and electronic form (e.g. cloud) or only hardcopy/only electronic form. Is it possible to have them stored on Cloud?
5. Please indicate whether there are any territoriality and duration requirements, i.e. whether the Upstream Data must be stored (either in hardcopy or electronic form) only within the boundaries of your jurisdiction or whether the data can be stored also abroad (outside your jurisdiction); if the answer is affirmative and the data can be stored abroad, are there any mandatory additional requirements regarding the existence of the originals / back-up (hardcopy/electronic) copies which must be located territorially in the jurisdiction? Is there a mandatory period applicable to the back up obligation, if the case?
6. Please indicate which is/are the competent authority (authorities) with attributions regarding Upstream Data and which are the main competences related to the manner in which the Upstream Data is stored, disclosed, physically protected, backed up
7. Are there drafts of legal acts which refer to the legal regime of the Upstream Data which are currently under public debate and which may come into force in the near future, especially in the context of the entry into force of EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union?

   As regards future legal enactments in this area (at Romanian or European level), we relied solely on information/drafts which are currently publicly available on official websites.

   We did not conduct any interviews, nor did we proceed with any inquiries in front of the competent authorities. The study does not include any assessment from a competition law perspective.

2.2. Description of the main legal acts applicable in Romania related directly and indirectly to Upstream Data

The main legal acts regulating in Romania the handling of Upstream Data are listed below:

a. Petroleum Law no. 238/2004 ("**Petroleum Law**"), in particular article 4;
b. Methodological norms for the application of the Petroleum Law, approved by Government decision no. 2075/2004 ("**Methodological Norms**"), win particular articles 1 to 15;
c. Law no. 182/2002 concerning the protection of classified information and national standards for the protection of information classified in Romania;
d. Government decision no. 585/2002 for the approval of the National Standards for protection of classified information in Romania ("**National Standards**");
e. Order no. 202/2003 regarding the approval of the List of information which represents classified information within ANRM, as updated afterwards ("**Order 202/2003**");
f. Government Decision no. 781/2002 regarding the protection of classified work information;
g. Government Decision no. 1219/2009 regarding the organization and

functioning of ANRM;

h. Order no. 16/2014 approving the INFOSEC - INFOSEC 2 Directive.

2.3. Legal framework in Romania

2.3.1. Legal ownership of the Upstream Data

According to the Petroleum Law, all data and information obtained from operations conducted in relation to Romanian petroleum resources and reserves is in the ownership of the Romanian State.

Such data and information obtained by the legal persons conducting petroleum operations may be solely used in their own interest. For the transfer of these data and information to other interested parties, a prior approval from ANRM is required.

Moreover, data and information held in the archives of the legal entities are confidential and will not be disclosed without ANRM's prior written approval. No express exception from the principle of obtaining the prior ANRM written approval is regulated under the Petroleum Law and its methodology.

2.3.2. Types of the Upstream Data

The Methodological Norms describe in more detail the types of upstream information, as follows:

- data on mineral resources and reserves obtained from mining and petroleum activities regardless of their storage mode represent the National Geological Fund („FGN");

- all resources and reserves identified and recorded by ANRM for each type of the country's petroleum resources represent the National Petroleum Resources/Reserves Fund ("FNR").

2.3.3. Security classification of Upstream Data

The data and information mentioned above belong to the Romanian State and are treated, as the case may be, either as (i) classified information or (ii) public interest information, according to the law.

The status of classified information triggers the obligation to observe certain rules regarding the access, protection and management of these data, rules applying not only to the public institutions, but also to the economic operators and the natural persons having these information in their possession.

2.3.4. Rights and obligations of oil operators and ANRM in relation with classified information

A. Acces to data held by ANRM and by the economic operators

The Methodological Norms expressly require information which form FGN and FNR to be kept, deposited and physically protected in ANRM's archives or in the archives of economic operators / public institutions which elaborated such or to whom such information is entrusted. Data and information from FGN and FNR which are classified are kept and deposited in the departments with classified information of the involved institutions, which must observe the physical security rules provided under the law.

Access to data and information must follow a strict procedure implying the below:

i. written request approved by ANRM;

ii. execution of an NDA and payment of the consultancy fees/data utilization fees

iii. access shall be granted within 10 days from date both conditions (i) and (ii) above are fulfilled.

The purpose grounding the request for access can be *e.g*. for the drafting of technical data, before the granting of the concession or during the existence of the concession. For access to data and information covered by an ongoing petroleum agreement, approval of the petroleum licensee is necessary as well.

B. Handling obligations of licensees

Licensees of petroleum agreements have the right to hold and use data and information related to perimeters subject to concession, during the existence of the petroleum agreements, for the purpose of performing the petroleum operations, with the observance of the conditions imposed by the legislation of classified information and of the contractual provisions regarding such data.

In this sense, licensees of petroleum agreements have the obligation to:

i. keep in its possession both the data and information given in its custody during the existence of the petroleum agreements, as well as those obtained through their own activity; and

ii. transmit the data in its possession to ANRM at the expiry date of the petroleum agreements;

iii. keep daily updated records of data and information in their possession, for each perimeter and transmit to ANRM copies of these, at the end of each calendaristic year, for their inclusion in the Oil Book;

iv. conclude with ANRM agreements having as scope the holding, depositing and security of the data and information which exist or which are obtained by the petroleum operators;

v. keep the data and information included in the scope of the agreements mentioned at point (iv) above deposited in a distinct place from the personal archives; if such data and information are classified information, the agreements mentioned at point (iv) must observe the specific legal requirements as well;

vi. obtain, as the case may be, the approval of the competent authority in the area of classified information; in this respect, the data and information held in their archives are confidential and their content cannot be disclosed without written approval of ANRM;

vii. cannot invoke a retention right over the archives containing the above mentioned data, which must be handed over to ANRM, at the location indicated by the later;

viii. elaborate the evaluation studies of the oil geological reserves and transmit them for verification and registration with ANRM;

ix. report annually to ANRM the existence, status and movement of the oil reserves/resources - separately, for each perimeter.

In addition, according to the Methodological Norms, in case of a foreign legal entity acting as petroleum operator, the original documents containing the data and information will need to be kept in the archive of the subsidiary located in Romania. The owner of the petroleum

agreement is however entitled to send copies of the data and information to its foreign headquarter, the headquarter of its operator or subcontractor located outside Romania, with approval of ANRM, for fulfilling its contractual obligations.

C. Rights of ANRM with regard to data and information

ANRM is entitled pursuant to the current legal framework to:

i. have a permanent access right to the data and information, irrespective of their place of depositing, in a freely and unrestricted manner; and

ii. control the manner in which the data is kept, deposited and protected, as well as the manner in which they are used by the owners of the archives.

D. Legal regime of classified information

Classified information has a specific legal protection regime due to its importance and sensitive nature. Currently, the legal framework tries to prevent any unauthorized access to such data, its alteration, modification our unauthorized destruction, as well as security of the informatics system. This can be achieved in a risk-orriented approach, by identifying situations and persons that through their actions can jeopardize classified information, as well as strictly limiting the personnel handling such data and providing physical protection to the data and information and to the personnel handling the data.

The National Standards are the legal act containing the general rules applicable for classified information state secrets. Note should be made that the standards have certain references to work secrets as well and, furthermore, GD no. 781/2002 mentions expressly that the provisions of the National Standards apply to work secrets as well, in matters related to:

i. classification, declassification and minimum protection rules;

ii. general rules for registration, drafting, maintenance, processing, transport and transmission;

iii. obligations of management of the public institutions and economic operators; and

iv. access of foreign citizens to classified information.

The protection of classified information includes: a) legal protection; b) protection by procedural measures; c) physical protection; d) protection of personnel with access to classified information or appointed to ensure its security; e) protection of information-generating sources.

E. Types of classified information

Classified information is of two types: (i) state secret (in Romanian, *secret de stat*); and (ii) restricted information/work secret (in Romanian, *secret de serviciu*); the main difference lies in the person/ entity that could be damaged in case of their disclosure / processing: in the first case, the national safety, in the second case, a legal public or private entity.

The lists with restricted information are established by the management of the organizations holding such information. Such lists must include information referring to the activity of the organization that, according to the law, is not qualified as state secret information, but should be known only on a need to know basis, by those persons

who require it in fulfilling their duties.

The class (in Romanian, atribuirea clasei) and classification level (in Romanian, nivelul de secretizare) of an information shall be assigned after consultation of the classification guidelines, of the lists containing the state secret information and the lists containing the "secret de serviciu" (restricted) information, drawn up according to the law.

F. ANRM restricted information list

According to ANRM Order no. 202/2003, the following information and data are regarded among others, as restricted information (in Romanian, *secret de serviciu*) in the oil and gas area:

Document	Classification period
Evaluation documentation of petroleum resources/reserves and gas, determined or estimated on knowledge categories, expressed by quantity and quality, at the level of each deposit, structure, formation, territorial administrative unit, region (point 2)	Permanent
Verification reports of evaluation documentation of resources/reserves, of technical economical studies and of justification of exploitation for (among others) oil and gas (point 4)	According to the classification of the evaluation documentation
The concession license for exploration, the related documentation elaborated thereof, annual / final reports (point 7)	5 years from termination (except if the information was part of a license)
The concession license for exploitation and its annexes (feasibility study regarding the valorification of the mineral resources and protection of the deposit and the development project of the exploitation) (point 8)	Until depletion of the deposit
Petroleum agreement and the documentation related thereof (point 9)	5 years from the termination of the petroleum agreement
Approval to the annual exploitation program and related documentation (point 13)	Until depletion of resources/reserves
Amendment approval to the annual exploitation program and related documentation (point 14)	Until depletion of resources/reserves
Information, data and geodesy documentation, topo-photogrammetry and mapping related to documentation classified as restricted (in Romanian, *secret de serviciu*) (point 16)	According to the documentation

Petroleum book and extracting cadaster shall be classified depending upon the nature of the content of the information which they contain (point 17)	Until depletion of the resource/reserve

G. Internal protection rules within the organization of an petroleum operator

Transmission of classified information to other users may be done only if they hold security clearance certificates or access authorizations appropriate for the required secrecy level. The managers of the entities handling classified information have the obligation to notify the competent institutions with control and surveillance competences in the area of any events out of which breaches of security may result.

- Security officer/special compartments

  Security structures with specific tasks shall be established, under the terms of the law, in organizations holding such information, for the implementation of the protective measures of classified information. In case the organization holds a small amount of classified information, the tasks of the security structure shall be fulfilled by the security officer.

  In entities holding classified information, special compartments shall be organized for recording, drafting, storage, processing, reproduction, handling, transport, transmission and destruction in secure conditions. The activity of special compartments will be coordinated by a security structure/officer.

  In addition, the security structure/officer has the following competences:

  i. drafting and updating the list of classified information elaborated and stored by the unit, on categories and secrecy levels

  ii. drafting of the program for preventing leakage of classified information and submission of the program for approval to the competent institutions;

  iii. coordination of the activity for protection of classified information.

- Access to information

  Access to information shall be provided internally (within the organization) on a need-to-know basis, to persons holding the security certificate / access authorization, valid for the level of secrecy of those information, required for fulfilling the job requirements. The same principle is applicable in case of transmission of the information between different entities.

  The heads of entities shall take the necessary measures of registering and controlling the classified information, **so that this could be located at any time.**

  According to GD 781/2002, it is forbidden to take out the restricted information from the unit holding the restricted information without approval of the management of the unit.

  Acces of personnel to restricted information is allowed only pursuant to a written authorization, issued by the management of the unit. Evidence of the access authorisations is kept by the

security structure/officer. Removal of the access rights are also made pursuant to a strict procedure regulated in the legal act.

Access of foreign citizens, of citizens with dual citizenship (Romanian and foreign) or of apatrid persons to the restricted information is allowed pursuant to the procedure included in the National Standars, based on a special access authorization and the need to know principle.

- Drafting of documents containing confidential information

  Drafting documents containing classified information must follow specific rules, specified in the National Standards at articles 41-50.

  For example, when classified documents are used as sources for other documents, the marking of the source documents shall determine those of the final document. The final document shall bear the mentions of the source documents used for their drafting. Number and initial registering date of the classified document shall be kept, even if the document is amended, until the secrecy class or level of the respective document shall be reassessed

  In all cases, the packages or supports for the storage of documents or materials containing classified information shall be marked with the secrecy class or level, the date and registering number and a list with their denominations shall be attached to them.

  Transmission of multiplied classified information is made mandatory with the approval of the security structure/officer, and the issuer will indicate clearly all restrictions associated with these information.

  GD 781/2002 has specific provisions tailored for restricted information/ work secrets, as follows:

  i. identification of documents regarded as restricted information / work secrets shall have after their identification number an "S" applied thereof, and on each page "restricted information" shall be included;

  ii. when constituted in folders, or tied in separate volumes, their cover and title shall contain the respective marks;

  iii. their evidence shall be kept separately from documents classified as state secret or unclassified.

- Special registries

  Records of material and documents containing classified information shall be kept in special registries, in compliance with the models provided in the Standards, in Annexes 4, 5 and 6. Each document or material shall bear the date and registering number from the record registries.

  Documents and materials containing classified information recorded in the registries mentioned above shall not be recorded in other registries. Originators and holders of classified information shall keep record of all the received or sent documents and of the documents drafted by the entity, according to the law.

  The name and surname of the person who has received the document shall be mentioned in the record registries for classified information, and the person shall sign for receipt in a recording

book.

Assignment of the same registering number to documents with different content is forbidden.

The registries shall be filled in by the designated person holding an appropriate security clearance certificate. Reproduction by typing and computer processing of classified documents shall be done only by authorized person with access to such information, only in specially designed rooms.

Specific references to registries for restricted information are also included in GD 781/2002.

- Other protection measures

  The management of the unit shall make sure that all persons handling the classified information are aware of the applicable legislation currently in force applicable in case of protection of classified information.

- Localisation of the classified information

  At any time the management of the units must ensure that all registration measures are taken in order to be able to establish at any moment in time, the palce where the classified information is located.

- Storing the classified information in electronic form/ electronic devices

  Classified documents may be microfilmed or stored on optical disks or magnetic supports under the following conditions:

  i. microfilming and storage is made, with the approval of the issuer, by personnel authorized for the secrecy class or level of the respective information;

  ii. microfilms, optical disks and magnetic supports shall enjoy the same protection as the original document;

  iii. all microfilms, optical disks and magnetic supports shall be specifically recorded and annually checked just like the original documents.

  The ways and measures for the protection of classified information in electronic format are similar to those on paper support. These measures and ways are expressly regulated under articles 236 - 337 of the Standards.

  As a general rule, the units handling classified information in electronic form must obtain an authorization (SPAD / RTD - SIC), by establishing a personal security strategy, for the purpose of being able to implement own security systems which shall include the utilization of specific products, trained personnel and protection measures, including control over the access to the informatics systems and services, on a need to know basis and the secrecy level. SPAD / RTD - SIC are undergoing regular evaluations, for the purpose of establishing the maintenance or withdrawal of the accreditation.

- Documents exiting the classification term

  Documents exiting the classification term are archived or destroyed. Their destruction shall be evidenced in a handover protocol.

- Declassification of confidential information

  i. State secret information

  State secret information shall be declassified by Government Decision, at motivated request of the originator.

  Information shall be declassified if:

  a. the classification period has expired;

  b. its disclosure shall not endanger national security and defence, public order or the interests of private or public legal persons holding it;

  c. the classification level has been assigned by an unauthorized person.

  Declassification or downgrading of state secret information shall be done by persons or senior officials authorized by law to assign classification levels, with prior notice of organizations coordinating the activity and controlling the measures for the protection of classified information according to their competence.

  Originators of state secret information shall periodically assess the need to maintain the secrecy levels previously assigned, and shall submit to the persons and senior officials authorized proposals as the case may be. Classified information determined as compromised or irreversibly lost shall also be declassified.

  ii. Restricted information

  "Secret de serviciu" information shall be declassified by the heads of the organizations originating it, by deleting it from the lists, which shall be reassessed whenever necessary.

2.4. Identification of key stakeholders

ANRM is the main competent authority in the oil and gas field, which ensures that the confidential Upstream Data belonging to the Romanian State is stored, transmitted, archived, processed and disclosed according to the legal provisions. More specifically, in this domain, ANRM coordinates the protection activity of classified data and approves regulations regarding the disclosure of the Upstream Data to third parties, with the observance of the specific legislation. In this regard, it has also a special department established for the fulfilment of this competence, namely the Classified Information Department (in Romanian, *Compartimentul Informaţii Clasificate*).

The department is established under the direct competence of the president of ANRM and has among others the following competences:

- drafting of internal norms regarding the protection of classified information
- drafting of the classified information leakage programe
- monitoring of the applicability and observance of the norms regulating the protection of classified information
- counseling of the managment of ANRM on classified information matters
- keeps evidence of the security certificates and the access authorisations to classified information
- drafts and updates the lists of classified information elaborated or kept by unit, class and secrecy level

- performs, with the approval of the management of ANRM, controls regarding the manner of applicability of legal measures for protecting classified information
- coordinates the activity for registration, drafting, storage, processing multiplication, use, transport, transmitting and destruction of classified information
- establishes a direction of security for information technology and communications, under its supervision, due to the fact that in the unity there is a system which automatically processes data where classified information is stored and processed.

SRI establishes (with the approval of the National Security Authority) the national standards for protection of classified information, which are mandatory. Among its competences, the following appear to be relevant in the context of the handling of classified information:

- to work out the national standards for classified information and their implementation objectives, in cooperation with the public authorities;
- to supervise the activities of public authorities for the implementation of this law;
- to provide specialized assistance for the programs designed to prevent the leakage of information drafted by public authorities and institutions, autonomous administrations and other companies holding such information;
- to control the manner in which the standards regarding the protection of classified information are observed and applied by the public authorities and institutions; e) to carry out checks and reviews of programs related to the protection of classified information, in certain locations;
- to organize, collect, transport and dispatch across the country the state secret mail and restricted official mail, in compliance with the provisions of the law;
- to assess and establish measures relating to the complaints and suggestions on the implementation of the programs for the protection of classified information;
- to identify any infringement of the norms on the protection of classified information, impose the contravention sanctions provided by the law, and notify the criminal investigation bodies in case of criminal offences.

2.5. Legal background at the level of the EU

Free flow of non-personal data means unrestricted movement of data across borders and IT systems in the EU. It is a key building block of the Digital Single Market and considered the most important factor for the data economy to unleash its full potential. The main legal act establishing the above rules is EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union (the "**Non-personal Data Regulation**")

The Non-personal Data Regulation aims to highlight that it is of the utmost importance that public authorities and bodies governed by public law to lead by example by taking up data processing services and that they refrain from imposing data localisation restrictions when they make use of data processing services.

The Non-personal Data Regulation applies to processing of non-personal data, which is any data that does not qualify as personal data under the General Data Protection Regulation 2016/679.

By "processing" the Non-personal Data Regulation means any operation or set

of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data localization requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality.

Member States shall immediately[1] communicate to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement. The regulation also mentions a deadline - 30 May 2021 - by which Member States shall repeal any existing data localisation requirement laid down in a law, regulation or administrative provision of a general nature and that is not in compliance with the principles included in the regulation. The Non-personal Data Regulation does not provide an explication for the term "immediately". Hence, the reasonable interpretation ist hat measures shall be taken as soon as practicable considering the object thereof, with the observance of the applicable deadline of 30 May 2021, same as for the obligation to communicate to the Commission an existing measure containing a data localization requirement (as per below).

By 30 May 2021, if a Member State considers that an existing measure containing a data localisation requirement is in compliance with the principles included in the regulation and can therefore remain in force, it shall communicate that measure to the Commission, together with a justification for maintaining it in force.

2.6. Principles in the implementation of the Non-personal Data Regulation

2.6.1. Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (COM/2019/250 final)

A first set of principles for the implementation of the new regulatory framework is set by the Commission in a guideline issued this year. The document ascertains that the trend at the level of the European Union, as outlined through the issuance and recent entry into force of the Non-Personal Data Regulation, is for enhancement of the legal certainty for businesses that they can process their data wherever they want in the EU, of the trust in data processing services and avoidance of vendor lock-in practices. There is a definite intention to increase customer's choice, improve efficiency and stimulate the adoption of cloud technologies, leading to significant savings for businesses in EU. Measures restricting the free movement of data within the EU can take various forms as they may be set out in laws, in administrative regulations and provisions or even result from general and consistent administrative practices.

Data localisation requirements shall be as a general rule prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality.

The prohibition of data localisation requirements covers both direct and

[1] *Art 4 alin 2: Member States shall immediately communicate to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in accordance with the procedures set out in Articles 5, 6 and 7 of Directive (EU) 2015/1535.*

indirect measures that would restrict the free movement of non-personal data.

- **Direct data localisation requirements** may be represented by territorial restrictions (*e.g*. an obligation of an operator to store data in a specific geographic location, for example if servers must be located in a particular Member State) or unique national technical requirements (e.g. data must use specific national formats).
- **Indirect data localisation requirements** do not have a standard form, as they can come in a variety of forms. They may include requirements to use technological facilities that are certified or approved within a specific Member State or other requirements that have the effect of making it more difficult to process data outside of a specific geographic area or territory within the European Union; the assessment of whether a specific measure represents an indirect data localisation requirement needs to consider the specific circumstances of each case.
- The exception from the general rule of free flow of non-personal data lies in the **public security**. Public security 'covers both the internal and external security of a Member State[2], 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[3], 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.
- Any data localisation requirement justified by public security reasons must be proportional. In accordance with the Court of Justice of the European Union's case law, the principle of proportionality requires that the **measures adopted are appropriate for ensuring that the pursued objective is met and do not go beyond what is necessary for that purpose**[4].

2.6.2. COMMISSION STAFF WORKING DOCUMENT, IMPACT ASSESSMENT, accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union

The document outlines from the first pages that a data's value (when it travels) can increase exponentially when it is aggregated, analysed, or used in innovative ways and it can become a competitive differentiator

[2] See for example the judgment of the Court of Justice of 23 November 2010, Land Baden-Württemberg v Tsakouridis, C-145/09, ECLI:EU:C:2010:708, paragraph 43 and the judgment of 4 April 2017, Sahar Fahimian v Bundesrepublik Deutschland, C-544/15, ECLI:EU:C:2017:225, paragraph 39.

[3] See for example the judgment of the Court of Justice of 22 December 2008, Commission of the European Communities v Republic of Austria, C-161/07, ECLI:EU:C:2008:759, paragraph 35 and case law referred to therein and the judgment of 26 March 2009, Commission of the European Communities v Italian Republic, C-326/07, ECLI:EC:C:2009:193, paragraph 70 and case law referred to therein.
In ruling C-161/07, the Court upheld that the only derogation under which the difference in treatment may fall is provided for in Article 46 EC, according to which discriminatory measures can be justified only on grounds of public policy, public security or public health. In that regard, even supposing that a danger of circumvention of the transitional rules governing the freedom of movement for workers from those eight new Member States is liable to interfere with the public policy of the Member State concerned, in the absence of proof by the latter to the requisite legal standard that the objective concerning the proper working of the labour market which is pursued by the legislation in question makes it necessary to put in place a general system of prior authorisation, applying to all economic operators concerned from those eight new Member States, and that that objective cannot be achieved by measures less restrictive of the freedom of establishment, the restriction on the freedom of establishment at issue is not justified.

[4] See for example judgment of the Court of Justice of 8 July 2010, *Afton Chemical Limited* v *Secretary of State for Transport,* C-343/09, ECLI:EU:C:2010:419, paragraph 45 and also case law referred to therein.

and an enabler for innovation and creation of new business models, for example in the fields of data analytics, text and data mining and app development. However, the document further specified that the possibility to build a data economy and to benefit from new technologies which rely on data is undermined by a series of barriers to data mobility, impacting business behaviour in the Single Market of the EU.

Such barriers are named „obstacles to data mobility", where „data mobility" refers to the degree in which data can be (re)located to different IT-systems, regardless of the physical location of such systems in the Union or the owner of such IT-systems, which might be the data holder himself or a data storage and processing/cloud service provider.

Among the problems which create such obstacles, the Commission verified the existence of the following four[5]: Member States' legislative and administrative restrictions, legal uncertainty, lack of trust and vendor lock-in.

(i) Legislative and administrative restrictions

Data localisation restrictions come in many forms, from legal provisions to administrative practices and they may be the effect not only of government measures, but also of regulatory authorities. This types of restrictions have been increased following the digitisation of the economy and the development of the data economy.

The main reason why Member States opt for such restrictions lies on (i) data security, referring to concerns like confidentiality, integrity, continuity and accessibility for the controller of the data, and (ii) the availability of data for supervisory and regulatory authorities of the Member States.

According to a separate study referred in the paper, security is often used as "convenient shorthand" for national security, national sovereignty and for security as a public policy task or as a protection of private interests. Therefore, some restrictions imposed in order to keep data out of reach of other jurisdictions and limit the access of other governments to specific types of data.

However, the paper further mentions that security concerns by Member States are largely unfounded, as localisation is not a proxy for security, but the means of storage is. Contrary to concerns on cyber security, evidence suggests that data stored in large-scale data centres is actually safer than data stored on-site. The economies of scale that are inherent to data centres make it easier to invest in state-of-the-art data security. In addition, cloud service providers spend much more time and effort on security to be compliant with certain certification schemes as to meet customer expectations and favour demand.

A number of the restrictions (such as the requirement to maintain data within a loction in order for the regulatory authority to have access to it) and requirements are based on considerations that originated in the 'paper era', where documents needed to be physically accessible for scrutiny or where only the original paper version had legal status. Despite the above mentioned reasons,

[5] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2017:304:FIN*

data localisation restrictions often are unjustified or disproportionate, since (i) effective alternative means to achieve the relevant public policy objective are available (e.g. requiring access to accounting and company data could replace outdated measures and obligations requiring accounting and company data to be stored locally) and/or (ii) the scope of a measure is excessive / the measure concerns non-critical data (e.g. requiring all public archives to be stored locally).

According to the OECD, computer services including data storage and data processing services are sensitive to restrictive regulations affecting trade and imposing an additional time burden on companies. It is crucial for these services to be delivered in a timely and agile manner. In view of the fact that all economic activities increasingly depend on them it is understandable why obstacles to such services *can* generate large economic losses.

(ii) Legal uncertainty and lack of trust

Legal uncertainty comes from the fact that in many cases the legal framework is rather ambigous or too many provisions must be corroborated in order to uderstand whether data can be moved or not. Besides this, the problem of lack of trust also constrains data mobility.

There is the broader category of lack of trust vis-à-vis certain types of data storage and processing as such (e.g. cloud computing). This type of lack of trust frequently originates from concerns over data security and the protection of sensitive data. It is still rare for customers to rely completely on cloud services for storing their valuable data. Fear of the risk of a security breach is the most common concern, which directly constrains the uptake of cloud services, and which in turn leads to efficiency losses for businesses and, ultimately, society as a whole.

Secondly, a lack of trust is seen when data localisation restrictions are adopted to ensure the availability of data for inspection/control purposes. The lack of trust surrounding jurisdictional and law enforcement challenges was also raised during the Structured Dialogues with the Member States in a workshop held in 2017. However, there is a solution, in the sense that localisation restrictions can be replaced with a functional requirement to ensure data availability for the supervisor, as the data can be made readily available for inspection electronically[6].

Consequences of data location restrictions

The consequences trigered by these problems are divided in four main categories: loss of growth/innovation potential, loss of operational efficiency, inefficiences in the data centres sector and market distortion.

According to responses to the public consultation, the highest impacts of data localisation restrictions are increased costs for business, limitation on the provision of a service to private or public entities or the ability to enter a new market (73.9% of responding stakeholders identified this impact as 'high'). The EU itself is perhaps the most compelling proof that the free provision

[6] This has been exemplified by the amendment to the Danish Bookkeeping Act 2015. Denmark now allows accounting records in electronic format to be stored anywhere without prior application or notification to the public authorities, subject to the requirement on the business to provide online access to the records held abroad at any time.

of services in an internal market leads to growth. Making the provision of cross-border data-based services in the single market more difficult would therefore put a constraint on the European economy.

The four policy objectives mentioned in the study are:

- Reduce the number and range of data localisation restrictions, enhance legal certainty and transparency of remaining (justified and proportionate) requirements;
- Facilitate cross-border availability of data for regulatory control purposes, specifically when that data is stored / processed in another Member State, reducing the propensity of Member States to impose data localisation restrictions for that purpose;
- Improve the conditions under which users can switch data storage and processing (cloud) service providers and port their data to a new provider or back to their own IT systems;
- Enhance trust in and the security of (cross-border) data storage and processing, reducing the propensity of market players and the public sector to use localisation as a default safe option.

2.6.3. Data location restrictions

One Deloitte study shows that businesses in EU can save 20-50 % of their IT costs by migrating to the cloud[7].

In the year 2017 a study[8] was finalised with the main purpose to provide an analytical framework that allows for a definition, mapping and understanding of various concepts of barriers to the free flow of data, both from a regulatory and non-regulatory perspective in 20 member states of the European Union.

The research team relied on two different types of barriers: direct and indirect barriers. While (i) a **direct barrier** is visible in a situation when a law (or other regulatory text) explicitly states where data may or may not be stored or transferred, or when the law contains an obligation that can only reasonably be met by keeping the data in a specific location and in case of unique national technical requirements (where the use of specific encryption technologies, data formats, accreditation procedures etc. which are inaccessible to foreign service providers are mandated), (ii) an **indirect barrier** is regarded as such when a law contains requirements that in practice are likely to be interpreted to restrict data location or data flows.

For example, a direct barrier could be triggered by a legal restriction for the data to stay in a specific country, in a specific building, in a specific data centre, while an indirect barrier could be reflected in a situation when (i) data must remain accessible to a supervisor or (ii) storage systems must be approved by supervisor or (iii) data may not be made accessible to third parties (iv) subcontractors must obtain prior approval or (v) Data must be destroyable in situation X or (vi) data must be kept on segregated systems.

From a qualitative point of view, within the research scope, a total of 40 barriers were identified, 30 of which were indirect, and 10 direct.

[7] Deloitte: Measuring the economic impact of cloud computing in Europe, SMART 2014/0031, 2016. Available online at: **http://ec.europa.eu/newsroom/document.cfm?doc_id=41184**

[8] https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market-study-data-location-restrictions

The researched domains included: health, financial, citizen data and company records, judicial and privileged data, tax and accounting and other (a broad residual category encompassing various types of data from the private sector (mainly from the gaming/gambling sector) and the public sector (mainly in relation to e-government in general)).

From a quantitative point of view, the study further investigates the additional costs to businesses and other organisations that might arise as a result of restrictions to cross-border data flow. Research examined how data can be digitally transferred across borders. This was necessary to investigate the additional costs associated with different transfer methods affected by restrictions to cross-border data flow. It was established that cloud services offer the only commercially viable transfer method in terms of volume data transfers and access by multiple users.

The study further mentions that any data location requirement must be red together with the underlying policy objective which grounds the requirement.

On the other hand, the study outlines that **there are also cases where a Member State may legitimately not wish to open certain data to EU-level storage options, providing as example cases of national security and police databases**. More specifically, when the principal concern of a Member State is that certain data is so critical that it may not be subjected to any sovereignty than one's own, no foreign data storage option will likely be satisfactory.One question put under scrutiny by the study is „in which cases should Member States be able to introduce barriers to the free flow of data?"

Based on the available data and on existing legal principles of EU law, the conclusion would appear to be that data location restrictions can be legitimate only to the extent that these requirements are objectively justified and proportionate in the light of this public interest objective. When such a justification could not be provided, **the requirement must be recast into a functional requirement, in accordance with the functional requirements translation table provided in the study**.

This exercise implies the screening and simplification of national laws, simplifying the requirements, by translating them into functional requirements, and, potentially, the establishment of coordination and harmonisation mechanisms between the Member States (in case the resulting functional requirements result in specific technical or operational requirements). These will likely vary from sector to sector.

Among the many examples quoted in the study, we picked the following:

- **Storage facilities must be within national borders, or they may be outside national borders but a copy must be made to a mirror system within national borders** - the objective behind the barrier is identified as „Ensuring accountability and verifiability". The study provides as a potential solution the following: „Clarification that the fundamental requirement is to ensure the integrity and auditability of the information. Local storage or mirroring a system is not the only way of achieving this goal.
- Another example of a transition from formal to a function requirement comes from Denmark. More specifically, the old Danish Bookkeeping Act provided that accounting data had to be stored in Denmark. Pursuant to a new amendment of the Bookkeeping Act,

financial records can be stored abroad in an electronic format, provided that the authorities have access to the data. Thus, this has become a functional requirement rather than a location requirement. There is no need for approval before sending electronic data outside Denmark, whilst under the former regime, such storage abroad was only permitted, subject to a separate dispensation from the Danish Business Authority.

Translation from formal into functional alternative requirements that would achieve the desired objective while minimising data location impacts must be done on the basis of the underlying policy objective.

The study quoted above mentions that most of the types of requirements can be grouped together and correspond to a specific public policy interest. However, this does not imply that implementation of barriers to the free flow of data in the specific cases always achieves their intended policy objectives. Although the policy objective may be legitimate, the implementation of barriers to the free flow of data may be ineffective or disproportionate in light of the intended objective. By way of a specific example, it is clear that accounting documents must be accessible to tax authorities. However, this legitimate policy objective does not imply that data must be stored locally.

The study also touches potential indirect barries identified in several member EU states, including Romania. As regards Romania, the study **refers to the legal framework applicable in case of classified information and the manner in which they can be transmitted**.

We hereby list the provisions (among others) which may be regarded as indirect barriers in Romania:

- Article 4 of Petroleum Law (which although is not expressly listed in the EU study, may be construed as imposing indirect barriers);
- Government Decision no. 585/2002 states that transferring classified information to other users requires security certificates and authorization access according to the appropriate level of secrecy.
- Top secret information cannot be stored, processed or transmitted in automatic information and/or communication systems which are actually or potentially exposed to users without security clearance. Every transmission requires repeated approval. Information and Communication System must have an authorization from the National Registry Office for Classified Information or its subordinate agencies.
- Updates and modifications to information and communication systems in absence of a human operator are forbidden. Annex no. 10/C describes the protection measures of the information systems which process data and classified information together with the protection measures of the building where these information systems are based.
- Government Decision no. 781/2002 stipulates the authorisation procedure for access rights which requires written authorization by the director of the unit which holds classified information.
- Law no. 182/2002 sets the need for mandatory cypher or other cryptographic elements established by competent authorities.
- Order no. 16/2014 describes the security operation

manners/approaches (for different types of classified information and related specific measures for security certificates and authorization certificates. It requires that information and communication systems handling classified information can use the Internet or similar public networks only subject to adequate cryptographic protection.

The object of the restrictions covers the following:

- Archiving requirements within the archive of ANRM and the economic operators
- The general rule that the information is located in Romania
- The information may be accessed only by person which have an access authorisation
- The transfer of the information is subject to ANRM's approval

2.6.4. Cross-Border Data Flows Enable Growth in All Industries

A study[9] starts by listing various multi-national companies from traditional industries, including oil and gas companies, which rely on data collected and transmitted from various locations they hold in various places around the world.

Further, the document mentions the issue of "data protectionism", for example location barriers, i.e. cross-border data flows are hindered due to data residency requirements that confine data to their borders.

In identifying the reasons supporting the data protectionism measures, motivations rely on such reasons as privacy and security of their citizens' data. But as shown in a previous report[10] that there is absolutely no increased privacy or security resulting from mandates that require data to not leave a nation. When it comes to data security, it does not depend on where the data is stored, but rather the means used to store it.

As regards the negative impact that such data localization barriers may bring on the economical activity of international legal entities / holdings, such are related to costs, raised prices for consumers and reduction of international competiveness of a firm. Not only firms are harmed by these types of measures, but also indirectly the state. An example for the oil and gas industry is detailed by the study mentioned above:

Furthermore, forced data localization would affect many mining, oil, and gas companies seeking to send their own information across borders. For example, data localization laws could prevent Shell from transmitting data from a site in one country to another, thereby barring it from using the massive amount of information it collects in its wells to paint a complete picture of its operations, information which can lower costs for consumers and reduce environmental impact. As Shell continues to embrace big data in its "Smart Fields," it may face data localization laws that focus on information that may be sensitive on national security grounds. In 2011, Shell moved its cloud storage from a U.S. provider to a Germany provider due to concerns about the U.S. Patriot Act. As a result of security fears stemming from U.S. surveillance, European countries such as Germany and the Netherlands have considered rules to prevent U.S. companies from offering their

[9] http://www2.itif.org/2015-cross-border-data-flows.pdf

[10] Daniel Castro, "The False Promise of Data Nationalism," The Information Technology and Innovation Foundation, December 2013, http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

services domestically.This would have severed Shell's relationship with Microsoft at the time. By creating barriers to cross-border data flows of international oil and gas companies like Shell, countries lose benefits such as better environmental monitoring, more efficient drilling, increased revenue from oil production, greater recoverable reserves, and increased local jobs due to expanded oil production.

In the recommendations and conclusions section, the study mentions that the use of cloud computing and data innovation has many positive benefits, including increased productivity and lowering costs of trade and hence the "battle" against data protectionism should be continued.

3. Analysis of foreign jurisdictions regimes for the data handling and preserving

3.1. Overview of legislation specificities of the four selected jurisdictions

3.1.1. Norway

(i) Main legal acts

- Act 29 November 1996 No. 72 relating to petroleum activities and the regulations issued in relation thereof.

(ii) Handling rules of Upstream Data

According to the Norwegian Petroleum Act[11], material and information which the licensee, operator, contractor etc. possesses or prepares in connection with planning and implementation of petroleum activities **shall be available in Norway** and **may be required to be submitted free of charge to the Ministry** or to anyone designated by the Ministry. Such material and information shall be submitted **in a format decided by the Ministry** to the extent this is deemed reasonable. In this connection, the Ministry may also require analyses and studies to be carried out. When a production license is surrendered, the operator takes over the responsibility for material and information relating to the surrendered production license according to this provision.

More specifically, pursuant to the Regulations to Act relating to petroleum activities[12], the licensee shall submit to the Norwegian Petroleum Directorate information on:

- the volume of petroleum produced and on the composition of the petroleum etc, also including test production and the extraction of petroleum in connection with formation testing;
- use, injection, cold venting and burning of petroleum;
- volumes and other results of monitoring, as well as monitoring procedures.

The Norwegian Petroleum Directorate may stipulate further provisions relating to reporting. The Norwegian Petroleum Directorate may require additional information.

The Regulations further regulate the transmission of information regarding sale of petroleum, plans and budgets, R&D projects, information from areas outside the Norwegian continental shelf.

Materials and information which the Ministry and the Norwegian

[11] Act 29 November 1996 No. 72 relating to petroleum activities https://www.npd.no/en/regulations/acts/act-29-november-1996-no2.-72-relating-to-petroleum-activities/#Section-10-4
[12] https://www.npd.no/en/regulations/regulations/petroleum-activities/

Petroleum Directorate may require to be submitted pursuant to the Norwegian Petroleum Act **also comprise software which is used to process the former, plus the necessary documentation in this connection**. The licensee **shall pay the transfer costs to the machines of the users to the extent this is considered reasonable**.

The licensee shall retain for safekeeping material and information necessary to ensure that the relevant authorities (*i.e*. Ministry) can verify whether the petroleum activities are carried out in accordance with the statutory framework of legislation, for as long as it provides necessary information about the petroleum activities.

If the operator wishes to destroy material or information which may be of importance to the management of resources, the Norwegian Petroleum Directorate shall receive a list of material and information prior to it being destroyed, and may within a reasonable time after having received the list order handing over or further safekeeping free of charge. In the case of handing over, suffcient documentation in relation to such material and information shall be included.

The licensee is obliged, through the operator, to make information about petroleum activities **publicly available to the greatest possible extent**[13] as and when such information becomes available to the licensee.

Information of any kind communicated to the authorities in connection with an application for production license shall be subject to duty of secrecy until the production license for the areas in question have been granted. Thereafter, as a general rule, the information shall be subject to duty of secrecy to the extent this is in accordance with the Norwegian public administration Act, for a period of 20 years.

3.1.2. Hungary

(i) Main legal acts

The main legal acts applicable in Hungary regulating the handling of Upstream Data produced by mining licensees are as follows:

- Act XLVIII of 1993 on Mining (hereinafter referred to as "Mining Act")
- Government Decree No. 203/1998 on the Implementation of the Mining Act
- Government Decree No. 161/2017 on the Mining and Geological Survey of Hungary (Mining and Geological Survey of Hungary in Hungarian: "Magyar Bányászati és Földtani Szolgálat"; hereinafter referred to as the "Mining Authority")
- Order no. 2/2017 of the President of the Mining and Geological Survey of Hungary

(ii) Legal regime of Upstream Data

Licencees are required by law to provide Upstream Data to the Mining Authority with the content and in the form prescribed by the Mining Act and its implementation decree.

Such Upstream Data subject to data provision obligation will be

[13] https://www.norskpetroleum.no/fakta/historisk-produksjon/

kept, processed, stored and archived by the Mining Authority within the Hungarian Geological, Geophysical and Mining Data Store (in Hungarian: "Magyar Állami Földtani, Geofizikai és Bányászati Adattár" hereinafter refererred to as: "Data Store") and will be classified into three main cathegories:

1. public data (in Hungarian: "nyilvános adat") - general rule, unless the information falls under the following two categories
2. business secret (in Hungarian: "üzleti titok")
3. data for preparation of decision (in Hungarian: "döntéselőkészítő adat")

(iii) Handling rules of Upstream Data

Order no. 2/2017 of the President of the Mining and Geological Survey of Hungary sets out the manners of the storage and accessibility of data kept in the Data Store.

In accordance with the three categories mentioned above, most of the geological, geophysical and mining data kept in the Data Store are accessible to the public, except for the data classified as (i) business secret and (ii) data for preparation of decision, regarding which the public has only limited access to.

1. Common rules applicable to the Upstream Data kept in the Data Store
   (i) Original documents cannot be removed physically from the Data Store.
   (ii) The requesting party cannot make notes in the original documents and cannot modify their state.
   (iii) The requesting party shall pay a fee to receive a copy of the original document.
   (iv) Borrowing an original document from the Data Store or forwarding any data kept in the Data Store to third parties is only permitted with the prior consent of the President of the Mining Authority.
   (v) The requesting party may forward the data accessed to its affiliates, branches or to a company of its business group indicating the rules restricting the use of such data.
2. Public data: All data kept in the Data Store qualifies as public data, unless such are qualified as restricted data.

   In order to access public data, a printed or electronic request for the access of data shall be submitted to the Mining Authority.

3. Restricted data (business secret and data for preparation of decision): Restricted data is only accessible with the limitations set out by the industry specific laws, the above cited order of the President of the Mining Authority and the relevant general act on information (Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information).

3.1. The following pieces of information provided by mining licencees shall qualify as business secret by law:

(i) data obtained in the course of exploration shall be treated as business secret until the termination of mining rights (or until the decision on the application for the establishment of the mining plot at the latest);

(ii) data obtained within the mining plot shall be considered as business secret until the termination of mining rights but, at the latest, for three years from the fulfillment of the respective data provision obligation;

(iii) the data provided by the exploration licencee for 1 year from the date of the resolution accepting the summarizing geological report;

(iv) in the case of the the geological data provided for the purposes of the common cultivation plan for three years following the fulfillment of the technical operational plan.

Such restricted data **can only be accessed if the owner of the data gives its consent**. The consent shall contain **the exact purposes of the use** of the data subject to the access request. The owner of the data in this relation shall mean the mining licensee who had previously submitted such data. In the case of business secrets, the requesting party shall obtain only the consent of the owner of the data to access the relevant restricted data. While in the case of data for preparation of decision, the requesting party shall obtain the consent of the President of the Mining Authority.

3.2. Data provided by mining licencees shall qualify as data for preparation of decision based on the decision of the Mining Authority if it serves as a basis of the Mining Authority's decisionmaking procedure.

The subject of the Mining Authority’s decision-making procedure may cover – *inter alia* - the designation of mining areas, granting mining concessions allowing exploration works, etc.

When making decisions regarding the above, the Mining Authority may rely on data and information previously submitted by mining licensees (*e.g*. exploration reports, geological sudies, production reports).

As a general rule, **such data shall not be made available to the public for 10 years from its creation.** Upon request, the president of the Mining Authority is entitled to grant access to such data under specific circumstances

provided that the underlying public interest in the keeping of such information from the public is less important than the interest in the accessability of such information.

The restriction of the access to such data for preparation of decision is necessary in order to secure the lawful operation of the Mining Authority as a body carrying out public service as well as to guarantee that its decision- making processes are functioning without interference. **These latter reasons are based on public interest and are explicitly set out in the relevant legislation**.

The industry specific Hungarian laws regulate only the manner and form by which the mining licencees are required to submit the Upstream Data to the Mining Authority but do not contain provisions on how the mining licencees are required to storage, process or archive such data.

As a general rule, the restriction stipulated in the relevant legislation apply to the Mining Authority and not the mining licensee. The reason behind is that the aim of the relevant legislative framework is to secure the proper level of accessibility of the data handled by public bodies, *i.e*. it does not intend to impose restriction on the private entities submitting such data. Consequently, once the mining licensee fulfilled the data provision obligations prescribed it can decide on the way and means it will handle such Upstream Data in the future.

Upstream Data may be provided to the Mining Authority in the way prescribed by the Mining Authority which may be:

(i) in hardcopy form or

(ii) in electronic form or

(iii) or by providing sample materials (soil sample, rock sample)

The relevant datasheets provided by the President of the Authority shall always be attached to the Upstream Data submitted.

In the same manner as described above, there are **no territoriality requirements on the storage of Upstream Data**. An exception is the requirement on the storage of sample material (soil sample, rock sample). Sample materials must be kept and stored by the mining licencees until the end of the exploration works (provided that the Mining Authority has imposed such obligation in the licence itself). Sample materials can only be disposed or destroyed with the prior consent of the Mining Authority.

Notwithstanding the above, it would be recommended to keep and storage all data concerning the Hungarian activities pursued by the mining licencees until the end of the general limitation period in line with the general Hungarian civil, tax and accounting law (5-7 years).

Furthermore, it cannot be excluded that the Mining Authority imposes special obligations concerning the storage of certain Update Data in its licence issued to the mining licencee.

(iv) Competent authority

The National Assembly of Hungary (in Hungarian: Országgyűlés) possesses the main legislative competences, and is, therefore, entitled to primarily regulate the fields of mining as well as freedom of information and data protection by way adopting laws.

The Government of Hungary (in Hungarian: Kormány) is entitled to create certain detailed rules of the above fields based on the specific authorizations of the relevant laws passed by the National Assembly.

The Mining and Geological Survey of Hungary ("**Mining Authority**") is the authority specifically responsible for the supervision of the mining industry in Hungary. The relevant competence of the Mining Authority includes *inter alia*:

i. the enforcement of national interest connected to the registration of geological data;

ii. enhancement of the level of exploration of the mineral resources in Hungary;

iii. collecting, processing, preservating and providing data generated in the course of geological, geophysical explorations and mining operations and the utilization thereof;

iv. collecting, processing, preservating and providing geological data generated in the course of assessment of geological hazards and the utilization thereof.

In line with the above, the Mining Authority issues the licences of the mining licencees and determines its exact content. The Mining Authority is also responsible for the operation of the Data Store. The President of the Mining Authority regulates the operation of the Mining Authority and the Data Store with internal orders (in Hungarian: utasítás).

The National Authority for Data Protection and Freedom of Information (in Hungarian: Nemzeti Adatvédelmi és Információszabadság Hatóság) is the authority responsible for securing the freedom of information and the effective protection of personal and other qualified data. The latter authority has the competence to ensure the accessibility of public data.

(v) Publicly available drafts of contemplated legislative acts

Based on publicly available information there are no drafts of legal acts which refer to the legal regime of the Upstream Data which are currently under public debate and which may come into force in the near future in relation to the entry into force of EU Regulation 2018/1807.

3.1.3. Italy

(i) Main legal acts

The main legal acts applicable in the Italian jurisdiction, regulating the manner in which Upstream Data is classified, kept, processed, transmitted, disclosed, archived by petroleum licensees are:

- Law 21 July 1967, no. 613 regarding "Research and cultivation of liquid and gas hydrocarbons in the territorial sea and on the continental shelf and amendments to Law 11

January 1957, n. 6, on the research and cultivation of liquid and gaseous hydrocarbons". In particular, article 39 specifies how to treat the techincal and economic data regarding the exploration, research and cultivation activities of hydrocarbons;

- Legislative Decree 6 September 1989 reagrding "Law provisions on the National Statistic Service". In particular artciles 7, 9 and 10 specify the obligations of the private entites involved in the research and cultivation of hdrocardons, to transmit the relevant data, in an aggregate form, to the Italian Minister of Economic Development (hereinafter "MISE");

- Legislative Decree 31 March 1998, no. 112 regarding "Functions and administrative tasks of the State to the regions and local entities". In particular the State, thorugh MISE, is the competente entity responsible for the collection of data of hydrocarbons. The entities having permits and concessions must transmitt data to the local Regions that will transmitt the same to MISE;

- Directorial Decree of 15 July 2015, regarding the modalities of the exploration, research and cultivation activities of liquid and gas hydrocarbons according to DM 25 March 2015;

- Ministerial Decree ("DM") of 7 December 2016, as amendend and integarted by DM 9 August 2017, representing the last Standard Disciplinary for permits of explorartion and research and cultivation concessions of liquid and gas hydrocarbons. In particular, it regulates the modalities regarding the treatment of data resulting from the permits and concessions terminated/revoked.

(ii) Legal regime of Upstream Data

The Upstream Data regarding permits and concessions terminated/revoked are considered public information.

With regard to Upstream Data concerning **permits and concessions still effective**, Article 53 of Directorial Decree of 15 July 2015 (that recalls article 39 of Law 613/1967) provides that the technical and economic data and information relating to exploration, research and cultivation, **provided to the administration by the licensees and concession holders**, **which are confidential** - such as geophysical surveys with related interpretations, geological profiles of wells with diagrams, related correlations, the extent of reserves - **may not be published (for example, in the Official Journal or other public registries) without the written consent of the relevant/interested parties**.

The term “administration”, mentioned in article 39 of Law 613/1967, refers to the Italian Minister of Economic Development (MISE) and the competent UNMIG Section (National Mining Office for Hydrocarbons and Geothermal Energy), which are the competent authorities that receive the information and documentation provided by the licensees and concession holders.

The term “interested parties” refers to the subjects

involved/mentioned/concerned in the confidential technical and economic data/information which can be affected by the publication of such data/information. The licensees and concession holders, as well as physical and legal entities operating in the research/ exploration/ drilling/ cultivation activities, can be included among the definition of "interested parties".

We have not identified similar restrictions for the licensees in keeping internally the data not communicated to MISE and UNMIG Section. According to article 39 of Directorial Decree of 15 July 2015, the confidential restrictions regard the data/information communicated by the licensees and the concession holders to the competent authorities above. The licensee and concessions holders can regulate internally the treatment of the data not disclosed covered e.g. by intellectual property rights.

(iii) Handling rules of Upstream Data

The Upstream Data regarding permits and concessions terminated/revoked shall be sent to the MISE within 6 months from the termination of the permits/title/concession. The Upstream Data above are made easily accessible to the public thanks to the ViDEPI web portal, created through collaboration between the MISE - National Mining Office for Hydrocarbons and Geothermal Energy ("**UNMIG**"), Assomineraria (Association of oil companies active in Italy) and the Italian Geological Society. ViDEPI web portal contains documentation concerning permits terminated since 1957 and filed with the UNMIG.

The archive of public data on the research and production of hydrocarbons in Italy that is the subject of the VIDIPI project is kept in hardcopy form at the library of the Roma Tre University.

The library manages the documentary material of technical and scientific interest concerning the research and production of hydrocarbons in Italy and in the sea territories to which it belongs. Administrative documentation and documentation still covered by the obligation of industrial confidentiality are excluded. The material preserved includes documentation from 1957 to the present day.

With regards to the permits in force, the Directorial Decree of 15 July 2015 details different type of reporting obligations, put in charge of the economic operators, regarding the communication of Upstream Data.

With reference to the **exploration permits**, article 19 provides **that the licensee shall send to the MISE and to the competent UNMIG Section a quarterly report on the progress of its operation works**. At the end of the operation or at the expiry of the exploration permit, the licensee shall submit to the MISE and to the competent UNMIG Section a final report, accompanied by all the seismic sections, in SEG-Y format (pre-stack and post-stack), indicating the operations carried out, the means and the teams employed and the results obtained. The transmission of documents and data may take place also in electronic format.

In accordance with article 22, the licensee for the drilling of the exploratory well shall inform the MISE and the competent UNMIG Section every six months of the progress of its operation works. The transmission of documents and data may also take place in

electronic format.

In accordance with article 22, **the holder of a research permit shall make available to the competent UNMIG Section**, the documentation in hardcopy or electronic format relating to the **searches carried out within the permit and the results obtained**, as well as the results of the layer and production tests carried out, the diagrams found in the well, and its own evaluation of the technical characteristics of production of the well itself.

With regard to the concession for cultivation and in accordance with article 34, the licensee, by the twentieth day of each month, shall submit to the MISE and to the competent UNMIG Section a report on the work carried out in the previous month and shall communicate the data relating to the production obtained. Within the first quarter of each year it shall communicate to the also the quantities of hydrocarbons produced and sent for consuming in the previous year.

Within the first quarter of each year, the holder of the cultivation concession shall submit to the MISE and to the competent UNMIG Section, in hardcopy and electronic format, an annual report updating the status of each licence, any further geomineral knowledge acquired during the previous year, the certified reserves and the updating of the production profiles, for each of the fields covered by the licence, and the consistency of the existing plants and equipment serving the licence on 31 December of the previous year.

In general, pursuant to article 53 of Directorial Decree of 15 July 2015, for all technical and economic data communicated by the various licensee to the MISE and to the competent UNMIG Section the provisions of article 39 of Law no. 613 of 21 July 1967 shall apply. In this regard, article 39 above provides that **the technical and economic data and information relating to exploration, research and cultivation, provided to the administration by the licensees and concession holders and which are confidential, such as geophysical surveys with related interpretations, geological profiles of wells with diagrams, related correlations, the extent of reserves, may not be made public (for example, in the Official Journal or other public registries) without the written consent of the parties concerned**.

We have not identified specific references in the Italian legislation about the reasons regarding the confidentiality of the information, e.g. public interest.

In addition, we have not found any specific regulatory provisions ruling the issues of territoriality for current concessions, but according to Directorial Decree 15 July 2015 referred in point 2) and 3) above, the licensees/concessionaires could transmit the Upstream Data in both hardcopy and electronic form. No references or prohibitions related to holding the information on a cloud server.

(iv) Competent authorities

With regard to the collection and processing activity of Upstream Data, the State (Italian Central Governament Authority), thorugh MISE and in particular thorugh UNMIG, is the competent

authority/entity, in accordance with article 33 of Legislative Decree 31 March 1998, no. 112. The economic operator holding permits and concessions must transmit the Upstream Data to the competent local Region authority, that will transmitt the same to MISE.

With the WebGIS system, the UNMIG makes available to all users the information regarding the exploration and production of liquid and gas hydrocarbons and the storage of natural gas.

The Upstream Data regarding permits and concessions terminated/revoked are made accessible to the public by vitue of the ViDEPI web portal, created through collaboration between the MISE - UNMIG, Assomineraria and the Italian Geological Society.

(v) Publicly available drafts of contemplated legislative acts

We are not aware about drafts of legal acts considered by the Italian Government regulating the legal regime of the Upstream Data in the context of the EU Regulation 2018/1807 on non-personal data free flow.

3.1.4. Poland

(i) Legal acts

- The Geological any Mining Law Act (ustawa prawo geologiczne i górnicze) dated 9 June 2011 along with executive regulations to this act.
- The Act on the Access to Information on Environment and its Protection, Society's Inclusion in Protection of Environment and on Assessments of Impact on Environment (ustawa o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko) dated 3 October 2008.
- The Act on access to public information dated 6 September 2001.

(ii) Legal regime

As a general rule, Upstream Data falls into the category of public information with **limited access**.

(iii) Handling rules of Upstream Data

The petroleum licensees need to provide geological information to designated authorities in a manner prescribed in executive regulations to the Geological and Mining Law Act.

The **State Treasury owns the rights to data that falls into the category of geological information within the meaning of The Geological and Mining Law Act.**

Generally, if the petroleum licensee developed the geological information, then it has the right to use it free of charge. The right to use the geological information is exclusive for the period of 3 years of receipt of the authority's decision approving the geological documentation containing the information. The exclusivity period is being extended if before the lapse thereof the licensee receives a decision to carry out upstream activities (for the period set in the decision and for additional 2 years of its expiry).

If the geological information was not provided by the petroleum

licensee and if it is to be used for prospecting and exploring of hydrocarbon deposits and extraction of hydrocarbons from deposits, than its use requires entering into a contract with designated authority with consideration.

Apart from restrictions on use of geological information (and apart from the obligation to provide the information to authorities) the regulations do not contain any provisions on how the data should be handled by the licensee. **Therefore the data can be stored, transmitted and named in a manner chosen by the licensee**. However if the licensee wishes for the information to be protected as its trade secret, than it needs to be able to show that this information was safeguarded.

In the field of processing and storing of the data the regulations focus solely on the obligations of authorities running the geological archives. **It is however not excluded that the licensee may be obliged by the agreement with the authority for the use of geological information to process or safeguard the information in a prescribed manner**. Should there be **special circumstances the authorities may also decide on classifying the data**. In such case the licensee would be obliged to handle it in a special manner describe in the Act on the Safeguarding of classified information.

If the Licensee is a **publicly listed company** than there are also regulations related to **the trading of securities**, which require some information (such as certain information on drilling by a PLC) to be kept secret under certain circumstances.

Also parts of geological information may fall under the category of environmental information, which should be disclosed upon request of interested parties.

Hence, unless there are no special circumstances (such as authorities classifying the information or the licensee agreeing a special manner of handling data in the cooperation agreement with concession authority regarding the use of information) there are no restrictions or requirements pertaining to storing of geological information.

In addition, notwithstanding the above, there are no express provisions regarding any territoriality and duration requirements, i.e. whether the Upstream Data must be stored (either in hardcopy or electronic form) only within the boundaries of your jurisdiction or whether the data can be stored also abroad (outside your jurisdiction).

(iv) Competent authority

The licensee is required to provide upstream geological data to the Ministry of Envirnment and to the State's Geological Service (Państwowa Służba Geologiczna). The State's Geological Service runs the geological archive, where it stores, physically protects and discloses the data.

(v) Publicly available drafts of contemplated legislative acts

Based on publicly available information there are no drafts of legal acts which refer to the legal regime of the Upstream Data which are currently under public debate and which may come into force in the near future in relation to the entry into force of EU Regulation 2018/1807.

4. Comparison between the legal regimes

4.1. Comparative analysis between the selected foreign jurisdictions

Data subject	Romania	Norway	Italy	Hungary	Poland
Ownerof the data	State	Owner of the licensee	The Legislation does not expressly identify the owner	The Legislation does not expressly identify the owner	State
Classification of data	restricted information (in Romanian, secret de serviciu	confidential	public data (regarding permits and concessions terminated/revoked) confidential (Upstream Data concerning permits and concessions still effective)	1. public data 2. confidential (the commercial data of the licensee and data for preparation of decision by the authority)	confidential
Storage and transfer formalities	only in Romania prior approval from ANRM for transfer within the territory of Romania prior approval of the owner of the license in certain cases	No requirements of form (hardcopy/electronic) or of territoriality. The only requirement is to have a copy in Norway.	No requirements of form (hardcopy/electronic) or of territoriality. Prior approval of the owners of the licensee in writing for transfer to third parties (except when the petroleum agreement stipulates otherwise)	No requirements of form (hardcopy/electronic) or of territoriality. Approval of the owner of the commercial data / owner of the license for confidential data Approval of the authority for data used in connection with the preparation of a decision of the authority	No requirements of form (hardcopy/electronic) or of territoriality. no express provisions with regard to transfer of data, data may be freely transferred by the owner of the license (except when the petroleum agreement stipulates otherwise))

4.2. Advantages and disadvantages of the identified regimes

The Romanian legal regime strictly regulates the legal regime of the Upstream Data as State owned data and structures the entire legal framework around this principle, thus requiring approval from ANRM for almost any process implying the processing of the respective data.

In opposition to that, the Norwegian legislator opted for a more flexible regulation of such data, in the sense that the data can be transferred to third parties more easily. However, at the same time, in order to provide constant access to the Norwegian authorities to this information, a copy must be permanently maintained in Norway. In this way, both interests (of the economic operator and of the competent authorities) are met: (i) the authority has constant access to the data and, at the same time, (ii) the economic operator has much more flexibility in processing or transferring the data.

A similar flexibility in matters of storage and territoriality requirements has been identified in Italy, Hungary and Poland, in the sense that there is no express requirement under their national laws to maintain/store the data in a certain form / for a certain duration / under a certain territory.

5. Identification of the trends in the EU legislation

No current project drafts of legal acts were identified in Romania, Hungary, Italy and Poland with respect to the modification of the legal regime of Upstream Data, elimination of bariers such as data localization or access to Upstream Data.

However, the general trend, as shown by the entry into force of the Non Personal Data Regulation and all the public studies mentioned in this study elaborated in relation with or in the context of the regulation show a tendency for openness of the non personal data flow.

The Non Personal Data Regulation establishes that by 30 May 2021, Member States shall ensure that any existing data localisation requirement that is laid down in a law, regulation or administrative provision of a general nature and that is not in compliance with the principles included in the regulation is repealed.

By 30 May 2021, if a Member State considers that an existing measure containing a data localisation requirement is in compliance with the principles included in the regulation and can therefore remain in force, it shall communicate that measure to the Commission, together with a justification for maintaining it in force.

6. Conclusions and recommendations. Potential improvements of the current national legislation

6.1. Conclusions

1. The tendency at European level is in the sense of removal / limitations of restrictions and barriers which exist at this moment in the member states of the EU with regard to the transfer, use, storage, processing and access of the data without personal character.
2. Apart from Romania, out of the analysed member states, we have not identified territoriality requirements for data specific to the Upstream industry;
3. In all the analysed states, the nature of the Upstream data is confidential, with several states including certain information in the public domain (the classification as „restricted information” (in Romania, *secret de serviciu*) (was not identified in any of the states).
4. In Romania, for the transfer of data it is necessary to obtain approval of

ANRM, while in the majority of states it is sufficient to obtain the consent of the owner of the license. Hungary imposes the approval of the competent authority for the category entailiing data used for justifying a decision issued by the authority.

5. There is a consensus at European level that openness towards technology is necessary for the economy of the EU, leading to growth of the productivity, competition and even ensuring the continuance of certain industry fields. In this sense, the Non personal Data Regulation was adopted.
6. Some member states within the EU have begun to eliminate data localization restrictions (Estonia, Denmark).

6.2. Recommendations. Potential improvements at national level.

1. Removal of unjustified barriers which take the form of localization data may trigger multiple operational advantages in all areas, including in the oil and gas industry:
   - easing access of the owner of the data and its users
   - increase of the cooperation between economic operators and authorities
   - optimization of the traceability of the persons which take contact with the respective data.
2. At a strategic level, adoption of new technology is the premises for creation of value, both for the Romanian State, as well as for companies from the oil and gas sector.
3. In the context of the obligation imposed by the European Regulation no. 2018/1807 on the member states ro reanalyze the legislation in view of removal of restrictions, it is recommendable to immediately consult the industries impacted by the respective restrictions.
4. The review of the legislative framework would lead to an increase of the interest of the investors in relation to the oil and gas upstream projects, to the creation of a national database to be further used for better substantiated energy policies, would ease the cooperation between the operators and the national authority. At the same time, the declassification of certain data would simplify the procedures at the level of the Romanian public bodies and may trigger a decrease in the number of the persons involved in the handling of such data.