Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

TMT
2022

Romania: Law & Practice
Alina Popescu, Daniel Alexie,
Flavia Stefura and Cristina Crețu
MPR Partners

Romania: Trends & Developments
Alina Popescu and Cristina Crețu
MPR Partners

practiceguides.chambers.com

ROMANIA

Law and Practice

Contributed by:
Alina Popescu, Daniel Alexie, Flavia Stefura and Cristina Crețu
MPR Partners see p.19

CONTENTS

1. CLOUD COMPUTING

1.1 Laws and Regulations

Overview

With the exception of certain provisions within the legislation concerning insurance and financial services, at present there is no legislation in force specifically regulating cloud computing. However, there have been regulatory initiatives from industry associations (eg, the National Association for the Security of Information Systems) in the form of guides with respect to, for example, cloud security.

In addition, there are certain legislative initiatives concerning the government cloud. In this respect, the Authority for the Digitalisation of Romania has been working on a draft enactment regarding the development of cloud infrastructure to be used by public institutions. The same authority is in the process of organising public tenders in view of the development of such infrastructure.

Cloud Services in the Financial and Insurance Sector

Cloud services are currently defined only in Romanian insurance legislation as services provided via cloud computing technologies to allow universal, convenient, on-demand network access to a common set of configurable computing resources, which can be quickly made available and launched with minimal effort of management from, or interaction with, the service provider. The said legislation also defines the following types of cloud:

- public cloud – IT infrastructure available for free use by the general public;
- private cloud – IT infrastructure available for use exclusively by one company; and
- hybrid cloud – IT infrastructure consisting of two or more distinct cloud infrastructures.

The legislation referred to above also imposes certain obligations that will be discussed below.

In addition, a guide on the externalisation to cloud services suppliers was released by the Financial Supervisory Authority in August 2021 for the attention of fund administrators and other entities that work with investment funds.

The guide applies from 31 July 2021 to all cloud outsourcing commitments concluded, renewed or modified on or after this date. The relevant entities are to review and amend existing cloud outsourcing commitments to ensure that they comply with this guide by 31 December 2022. In a nutshell, relevant companies must allocate clearly delineated responsibilities for managing outsourcing contracts. Furthermore, they must monitor the outsourcing contracts on a risk-approach basis.

In the insurance sector, specific norms implement the guidelines on outsourcing to cloud service providers of the European Insurance and Occupational Pensions Authority. Companies are subject to an obligation to evaluate their cloud outsourcing partners, in terms of risks posed by the cloud outsourcing activity. Insurance companies are also obliged to document their outsourcing relations in a separate registry where the information must be kept for two years after the contractual relationship with the outsourcing partner has ended.

The said norms on cloud outsourcing also provide minimum contractual provisions that must be included in the cloud outsourcing agreements. Insurance companies are obliged to ensure that cloud service providers comply with legal requirements and appropriate security standards.

All critical and significant outsourced cloud operations must be notified in writing to the Financial Supervisory Authority.

Data Privacy Aspects

Processing personal data in a cloud falls under the principles stated in the General Data Protection Regulation (GDPR).

Considering the Guidelines 07/2020 on the concepts of controller and processor in the GDPR issued by the European Data Protection Board (EDPB), the cloud providers mainly act as processors (ie, processing personal data under the instructions and on behalf of the controller), even where they offer standardised cloud services. In all cases where cloud providers act as processors, the parties must conclude a data processing agreement setting forth the conditions of the processing.

Following the invalidation of the EU-US Privacy Shield through the decision of the Court of Justice of the European Union in Schrems II, special attention should be paid to the transfers of personal data to third countries.

Whilst the first step is to ensure that the personal data is stored and processed entirely within the European Economic Area, due to the potential extraterritorial effect of surveillance laws governing third countries, the standard transfer tools provided by the GDPR might not be sufficient.

In this respect, the EDPB issued recommendations on supplementary measures to be used to ensure that the transferred data benefits from the same level of protection as that ensured in the EU.

2. BLOCKCHAIN

2.1 Legal Considerations

Overview

The only Romanian enactment referring to blockchain consists of technical norms for the implementation of blockchain technology in the computing system for the monitoring of voting turnout and prevention of illegal voting, as well as in the computing system for the centralisation of data from the minutes on the recording of voting results. These were enacted in November 2020.

Thus, while there is no general legal framework on blockchain, Romania has showed interest in implementing the technology and it can only be expected that further legislation will be enacted in the future.

For instance, there are signs that the National Bank of Romania (NBR) will join other European central banks in regulating cryptocurrency. In this context, it can be expected that the NBR will issue financial regulations that touch on blockchain technology in the future.

Risk and Liability

When it comes to blockchain, particularly open-source blockchain, it may prove difficult to identify the liable party when issues occur.

Depending on the level where the underlying issue occurs and the specific nature of the issue, liability could be imposed, for example, against one or more nodes in the blockchain and against the developer or the supplier of the software granting access to the blockchain.

Depending on the same, the risks and liabilities can be:

- of a contractual nature (eg, in the case of software suppliers);

- of a tortious nature (eg, a software developer that has no direct contract in place with the end user could be liable for a software flaw that has caused damages to the end user and be excluded under the contract between the software supplier and the end user); or
- of a compliance/public nature (eg, illegal activity undertaken via blockchain technology by any participant thereto).

In view of the above and the rather complex nature of blockchain technology, all the parties involved, whether it be nodes, software developers or suppliers or other entities providing various services based on blockchain technology, should assess their involvement and role in the blockchain and any potential issues that may occur at said levels so as to minimise risks and liability.

While not directly regulated under Romanian law, general norms under the Civil Code should enable any interested party residing in Romania to identify the competent court in which to claim compensation.

Nevertheless, specific legislation on blockchain would be welcome.

Intellectual Property

Blockchain is not expressly covered by Romanian legislation on intellectual/industrial property.

However, as blockchain essentially is a system that records information, it may potentially be argued that blockchain amounts to a database, which would make it subject to intellectual property rights.

At the same time, as blockchain technology can itself be used to record/register other assets to which intellectual property rights are attached, future enactments on blockchain may potentially encompass intellectual property aspects.

Data Privacy

Due to the nature of blockchain technology, the following data privacy-related aspects are of particular interest:

- identifying the data controller processing personal data of data subjects using blockchain-based products, such as cryptocurrency; this is since, due to its technical nature, all data uploaded by its users in the blockchain is processed by all nodes (such as miners) in the blockchain together; and
- enabling data subjects to exercise their rights, particularly the right to be forgotten, which might prove difficult in view of the way the blockchain works; where an individual has requested the deletion of their personal data from the blockchain, this would mean that all nodes would need to rebuild the blockchain from the moment the data subject to the deletion request was added, without including this particular data.

In view of the above, specific guidelines on how such data protection rights may be exercised should ideally be developed at European level. To this end, the European Data Protection Board has included within its strategy for 2021–2023 the assessment of new technology, including blockchain, as one of the key actions to be implemented.

Service Levels

As blockchain technology is not regulated in Romania, service levels should normally follow general contractual principles imposed under the Romanian Civil Code. Thus, services should be provided within the timeframe, under the conditions and at the price provided in the relevant supply contract.

Due to its characteristics, blockchain technology is considered an essential service per Romanian Law No 362/2018 on ensuring a high common

level of security network and IT systems. This encompasses services provided in the following essential areas: (i) energy; (ii) transport; (iii) the banking sector; (iv) financial market infrastructure; (v) the health sector; (vi) supply and distribution of water; and (vii) digital infrastructure.

If blockchain technology were to be used in one of the areas mentioned above, the supplier thereof would need to meet security and technical measures specific to essential services, as follows:

- access rights management;
- user awareness and training;
- journaling and ensuring the traceability of activities within computer networks and systems;
- testing and evaluating the security of computer networks and systems;
- management of network and computer systems configurations;
- ensuring the availability of the essential service and the operation of computer networks and systems;
- management of the continuity of the operation of the essential service;
- user identification and authentication management;
- incident response;
- maintenance of computer networks and systems;
- external memory media management;
- ensuring the physical protection of computer networks and systems;
- implementation of security plans;
- ensuring staff security;
- risk analysis and assessment;
- ensuring the protection of products and services related to computer networks and systems; and
- vulnerability management and security alerts.

Jurisdictional Issues

While blockchain technology is cross-border by nature, as the nodes thereof can be located in any country around the world and thus, at first glance, it may seem difficult to pinpoint the exact applicable jurisdiction, in the end this is achievable depending on the actual nature of the relevant dispute.

For example, when it comes to contractual relationships (eg, those between an entity providing blockchain-based software as a service and its end user, or between the licensor of such software and the licensee) between EU nationals/companies, where the parties have not established the applicable law, the same will in principle be the one of the country where the service provider/licensor has its habitual residence/registered office, in line with Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

In case of tort resulting from the use of blockchain technology, the applicable law would normally be the one of the countries in which the damage occurs.

When it comes to compliance matters, the applicable law would be determined according to the jurisdiction of the enforcers of the legislation infringed. For example:

- in data privacy matters, the applicable legislation would be that of the main establishment of the party found liable;
- in competition matters, enforcers would in principle have jurisdiction whenever an infringement had an effect on their respective territories; and
- in anti-money laundering matters, enforcers would have jurisdiction whenever money-laundering deeds are committed in their respective territories.

Consumer Protection

One other topic to be explored is whether and when blockchain users who are individuals could be considered consumers and hence, whether and when consumer protection authorities would have jurisdiction over potential complaints from such users.

For example, when purchasing and selling cryptocurrency, it is debatable whether an individual acts as a consumer or as a professional from a Romanian law perspective. Depending on the purpose of the activity concerned, either qualification may apply. For example, if such activity is performed for personal investment/savings purposes, in particular via a third party providing financial management/advisory services, it is more likely that the former qualification will apply. However, if the activity starts to be carried out directly and on a regular basis and/or on behalf of other persons who would be charged for the same, the individual may be deemed as a professional.

It is important to determine whether an individual acts as a professional or as a consumer, as in the second scenario the provider of the blockchain services/technology will need to consider the identity and comply with the rights of consumers applicable in their country of residence, for example:

- to provide the consumer with all information pertaining to the main characteristics of the provided services/technology in an easy-to-understand manner;
- to conclude a written agreement with the consumer pertaining to the provided services/technology that is easy to understand;
- to provide the consumer with information on all fees and costs pertaining to the relevant agreement to be concluded with the same; and
- to undertake that any and all amendments to the agreement concluded with the consumer can be implemented only upon the written acceptance thereof by the consumer.

Moreover, in such a scenario, according to EU and Romanian law, the agreement shall in principle be governed by the law where the consumer has its habitual residence, provided that the supplier pursues their commercial activities in such country or directs their activities to that country.

3. LEGAL CONSIDERATIONS FOR BIG DATA, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

3.1 Challenges and Solutions

Big data, machine learning and artificial intelligence are currently not regulated in Romania. Nevertheless, there is increased interest from certain authorities in relation to these fields.

Big Data

Competition

In 2021, the Romanian Competition Council published a document called a "Study on the effects on competition of the usage of Big Data platforms" (the "Study").

The need for the Study arose both from the rapid evolution of digital markets and the impact of big data on the economy. The absence of sufficient information in that respect caused the Romanian Competition Council to start working on the Study in 2018.

The Study has identified not only the strengths and opportunities arising from the use of big data (ie, economy of time and resources, innovation, efficiency and productivity, real-time information) but also the threats posed by such usage (ie, in

the area of data confidentiality, data protection, legitimacy of data usage and control over data quality).

Following the Study, the Romanian Competition Council concluded that, despite the positive impact of big data on economic growth (mainly through increased productivity and efficiency), the same has the potential to affect competition through abuses of dominance, by restricting or refusing access to data, or through collusion.

Intellectual property

In relation to intellectual property, one issue is whether algorithms used in big data can be protected through intellectual property rights. The answer so far seems to be that such algorithms are excluded from protection under European copyright laws, since "ideas, procedures, methods of operation or mathematical concepts" are not protected under EU copyright rules.

Patent protection of algorithms is also excluded. However, to the extent algorithms are used in the creation of computer-implemented inventions that are new, involve an inventive step and are susceptible to industrial application, the possibility of patentability, although still uncertain, is not excluded.

It is debatable whether algorithms can benefit from sui generis protection under database protection laws. In order for such protection to be granted, substantial investments must be made in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. It is unclear whether protecting algorithms can be linked to their role in obtaining or evaluating data.

Algorithms may, however, be protected as trade secrets, as long as they remain secret. However, the lack of transparency in algorithms creates its own set of issues, especially in the context of automated decision-making.

Another issue raised by AI algorithms is that of authorship. In Europe, the European Patent Office has refused two patent applications on the grounds that a machine, instead of a human, was named as inventor. This line of reasoning is likely to be followed by countries such as Romania.

Data privacy

The GDPR is based on observing key principles, such as lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, integrity and confidentiality.

At the opposite end, big data implies:

- collecting a huge amount of information;
- combining data from various sources; and
- further usage of the data in order to analyse and make decisions based on it.

Thus, ensuring that big data does not infringe GDPR principles can be a challenge.

Given the significant volume of information scattered across multiple systems, a company must have in place procedures and mechanisms enabling the swift location, extraction, rectification, restriction and/or erasure of the personal data concerned.

Artificial Intelligence and Machine Learning (as a Subset of AI)

National strategic framework

Romania has plans to develop a "national strategic framework in the field of artificial intelligence" through the project "strategic framework for the adoption and use of innovative technologies in public administration 2021–2027 – solutions for business efficiency".

In 2021, as a first step in the development of the national strategic framework, the Romanian Authority for the Digitalisation of Romania (ADR) in partnership with the Technical University of Cluj-Napoca launched a public consultation on AI. The public consultation was open to academia, businesses, consumers, professionals, and public sector entities that work with AI or for which AI represents a strategic element in the further development of Romania. The purpose of the public consultation has been to obtain qualitative data on the respondents' view of AI.

This initiative is in line with the European vision on AI, especially in light of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (the "Artificial Intelligence Act") and amending certain union legislative acts.

Competition

The Romanian Competition Council's Study referred to above concluded that, due to the ability of machine learning to learn constantly and adapt following the processing of real-time data, there is a risk of collusion between companies using such machine learning, for example, based on the rapid adaptation to a competitor's prices. However, in order for a cartel to exist, the will of more than one undertaking in this regard must still exist.

Intellectual property

Please see the section above regarding big data for potential intellectual property aspects, equally touching on AI.

Data privacy

In April 2021, the European Commission put forward a Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (the "AI Proposal") with an aim to provide a co-ordinated European approach on the human and ethical implications of AI.

Given the substantial reach of the data protection rules when dealing with AI, the EDPB and the European Data Protection Superviser (EDPS) have already expressed their concerns with regard to the content of the AI Proposal.

In this respect, the two European authorities underlined the need for the AI Proposal to expressly state that the data protection legislation in force applies to all processing of personal data which falls under the scope of the AI Proposal.

At the same time, given the high risks posed by the identification of natural persons in public places by using remote biometric techniques, both the EDPB and EDPS called for a general ban on using AI, which allows for automated recognition of human features in public places. The same ban should apply where AI systems use biometrics to clusterise individuals on grounds such as ethnicity, gender, and political or sexual orientation.

The EDPB and EDPS also call for a prohibition against using AI:

- in order to infer human emotions, except for specific cases where the recognition of emotions plays an important role for health reasons, such as health purposes; and
- for any type of social scoring.

Civil liability

As mentioned above, there are currently no specific rules with regard to AI. Thus, the general rules on civil contractual liability and tort law, as well as on administrative liability apply, the assessment being done on a case-by-case basis.

For instance, under the Romanian Civil Code there is an obligation for one party to repair the damages incurred by another party as a result of the use of an object. The liability sits with the person who owns or has control over the object or who uses the object in their own interest. Such person would be held liable, whether or not there was any fault on their behalf.

It is thus not unlikely for a person owning or using AI tools to be held liable for any damages that might result from events caused independently by the AI program, even if the latter did not receive a direct instruction to that specific end.

4. LEGAL CONSIDERATIONS FOR INTERNET OF THINGS PROJECTS

4.1 Restrictions on a Project's Scope

At the moment, the internet of things (IoT) is not regulated in Romania.

Nevertheless, when implementing IoT projects, one must bear in mind various pieces of legislation, examples of which are given below.

Data Protection

As IoT products generally collect and process large quantities of personal data, every such product should be thoroughly assessed to ensure its compliance with GDPR requirements, including those referring to data processing impact assessment (DPIA).

The Romanian National Supervisory Authority for Personal Data Processing has put large-scale processing of personal data generated by sensor-based devices transmitting data through the internet or through other means (IoT applications, such as smart TVs, connected vehicles, smart metering, intelligent toys, intelligent cities or other such applications) on the list of data-processing operations for which conducting a DPIA is required prior to deployment.

Cybersecurity

As the IoT implies the use of new technology that may be subject to security vulnerabilities, IoT-based projects might also need to consider compliance with cybersecurity legislation, such as:

- Law No 362/2018 on ensuring a high common level of security of networks and information systems transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the European Union (the "NIS Directive"); and
- Regulation (EU) 2019/881 of the Parliament and of the Council of 17 April 2019 on ENISA (the "European Union Agency for Cybersecurity") and on information and communications technology cybersecurity certification and repealing of Regulation (EU) No 526/2013 (the "Cybersecurity Act"), which was directly applicable in Romania as of 28 June 2021.

The Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the EU, repealing Directive (EU) 2016/1148 (the "Proposal") introduces the concept of "important entities" and adds new sectors where such important entities operate that would fall within the revised scope of the NIS Directive. One of such sectors is the manufacturing of certain critical products, such as:

- computer, electronic and optical products;
- electrical equipment;
- other machinery and equipment not elsewhere classified;

- motor vehicles, trailers and semi-trailers; and
- other transport equipment.

To this end, upon adoption and entry into force of the Proposal, the manufacturers of IoT devices that fall under the scope of the same will need to take key risk-management measures to manage risks to the security of network and information systems.

5. CHALLENGES WITH IT SERVICE AGREEMENTS

5.1 Legal Framework Features

In Romania, IT service agreements are not subject to specific laws, but rather to general contract law and various compliance requirements (data privacy, competition, cybersecurity, etc.)

The Romanian Civil Code regulates how contracts are concluded, executed and terminated. Due to the specificity of IT services agreements, the agreement should regulate in detail all relevant aspects which are not caught by general legislation or which need to be derogated from. One aspect that cannot be adjusted, however, refers to liability waivers, as Romanian legislation allows same only as regards monetary damages and only to the extent these were not caused by severe negligence.

Copyright

One noteworthy aspect in relation to copyright is that, according to Romanian law, the legitimate user of a computer program is allowed to correct errors in the program. This means that the program can be corrected even by third parties without authorisation from the copyright holder.

The legitimate user of the computer program or a person acting on their behalf may also reverse-engineer the program for the purpose of making it interoperable with other programs, without requiring the permission of the copyright holder.

Tenders

In public procurement procedures, the tender book usually has the contract template that will be signed attached to it. Therefore, negotiating such agreements or having the same amended is only possible to a minimal extent.

Banking

In the banking sector, to the extent that the IT services agreement is such that the IT services provider has access to confidential data regarding the clients or other data regarding the activities of the bank, the agreement is deemed as outsourcing, and is subject to specific regulations. The outsourcing contract with a credit institution must:

- clearly define the outsourced activity;
- establish the specific quantitative and qualitative requirements regarding the development of the outsourced activity, which would allow the credit institution to evaluate if the provision of services is adequate;
- have clear provisions of the rights and obligations of the credit institution and of the external provider, aiming also to ensure the observance of the law and of the prudential regulations during the contract;
- include a termination clause, which would allow the transfer of the activity to another external provider approved by the credit institution or its re-inclusion within the credit institution;
- include provisions regarding the protection of confidential information, the processing of such information and the maintenance of banking secrecy by the external provider;
- include provisions regarding the monitoring and permanent evaluation by the credit institution of the manner of execution of the

contract by the external supplier, so that it can promptly take any necessary measures;
- establish the obligation for the external provider to allow full access to its data/information in connection with the outsourced services, the internal audit function and the compliance function within the credit institution, respectively to allow, without restrictions, inspection and audit of the respective data by the financial auditor of the credit institution;
- establish the obligation of the external provider to allow, in connection with the outsourced services, the NBR to have direct access to its data, as well as to allow performance by the NBR of on-site inspections;
- provide for the need for approval of the subcontracting by the credit institution; and
- include a clause of unilateral termination at the initiative of the credit institution, including in case termination of the contract is requested by the NBR.

6. KEY DATA PROTECTION PRINCIPLES

6.1 Core Rules for Individual/Company Data

Core Rules regarding Data Protection

The core rules applicable in Romania as regards data protection are those under the GDPR, which is directly applicable in Romania.

In addition, Romania has adopted Law No 190/2018 on GDPR implementing measures ("Law 190/2018"), which regulates a series of measures regarding Article 6 paragraph (2), Article 9 paragraph (4) and Articles 37–39, 42, 43, 83 paragraph (7), 85 and 87–89 of the GDPR.

The implementation measures refer to, among others:

- the processing of genetic data, biometric data, or data concerning health for automated decision-making or profiling; the processing of such data should be done based upon the explicit consent of the data subject or an express legal provision, and with the establishment of appropriate measures for safeguarding the rights, freedoms and legitimate interests of the data subject;
- the processing of national identification data (personal identification number, identity card's series and number, passport and driver's license number, health social security number) and the collection or disclosure of the documents that contain the same; where the processing of such data is based on legitimate interest, certain warranties must be put in place by the controller or the third party processing the data;
- data processing in the context of employment;
- certain warranties that should be implemented for the processing of personal data and of special categories of personal data in the context of fulfilling a task carried out in the public interest;
- where the used data has been explicitly made public by the data subject or such data is closely linked to the capacity of the data subject as a public person or to the public character of the data subject facts, the same can be processed for journalistic purposes or the purpose of academic artistic or literary expression;
- the fact that, subject to certain warranties, political parties, non-government organisations of citizens belonging to national minorities and other non-government organisations are allowed to process personal data and special categories of personal data without the consent of the data subject; and

- the fact that public authorities and bodies that are found in breach of GDPR provisions must firstly implement the remedy plan provided by the National Supervisory Authority for the Processing of Personal Data; failure to implement the measures in the remedy plan can be sanctioned with a fine of up to RON200,000 (approximately EUR40,437).

Distinction between Companies/Individuals

Romanian data protection legislation (ie, the GDPR and Law 190/2018) does not apply to the processing of data concerning companies. Nevertheless, data belonging to companies may be considered trade secrets.

Data may be considered a trade secret if it meets the following conditions:

- it is secret in the sense that it is not, as a whole or as presented or articulated, generally known or easily accessible to persons in circles who normally deal with the type of data in question;
- it has commercial value; and
- it has been subject to reasonable measures taken by the person (company) lawfully in control of the data in order to be kept secret.

Misappropriation of clientele of a company by a former or current employee/representative or by any other person by using trade secrets is considered unfair competition and is subject to fines of up to RON50,000 (approximately EUR10,000).

Moreover, the disclosure, use or sale of trade secrets by a third party as a result of an act of commercial or industrial espionage, leading to the interests or activity of an entity being affected, is a crime punishable by imprisonment between three months and two years, or by a criminal fine.

General Processing of Data

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, which ensures that organisations are able to store and process non-personal data anywhere in the EU, is directly applicable in Romania.

Moreover, Law No 109/2007 on the reuse of information from public institutions ("Law 109/2007") regulates the conditions for publication and reuse of information existing in public institutions' databases.

Thus, the reuse of documents (and non-personal information reflected therein) held by public institutions is generally allowed.

To reuse such documents, the interested party must make a request reflecting the following:

- the public institution to which the request is addressed;
- the requested information/data, to enable the public institution to identify the relevant document(s);
- the identification details of the applicant; and
- the purpose for which the requested information/data will be used.

Such request may be:

(i) fully accepted by the relevant public institution;
(ii) partially accepted by the relevant public institution; in such a scenario, the public institution will need to motivate why the requested information was only partially disclosed and will need to provide the applicant with the possibility to challenge such partial refusal of disclosure; or
(iii) refused, where the same principles mentioned in point (ii) above apply.

Processing of Personal Data

Processing of Personal Data is regulated under the GDPR and Law 190/2018 mentioned above.

Other provisions applicable to processing of personal data are provided from time to time in specific legal enactments (eg, in legislation on the prevention and combating of money laundering and terrorism financing). Nevertheless, such provisions are secondary norms and follow the general principles and requirements under the GDPR.

7. MONITORING AND LIMITING OF EMPLOYEE USE OF COMPUTER RESOURCES

7.1 Key Restrictions

Law 190/2018 lays down specific conditions that apply where electronic monitoring and/or video surveillance systems are used in the workplace for the processing of employees' personal data, in order to achieve the employer's legitimate interests.

Such processing activities are subject to the following specific conditions:

- the legitimate interests pursued by the employer are duly justified and prevail over the interests or rights and freedoms of the data subjects;
- the employer has carried out the mandatory, complete and explicit informing of the employees;
- the employer consulted the trade union or, as the case may be, the representatives of the employees before the implementation of the monitoring systems;
- other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proved to be effective; and
- the retention period of the personal data is proportionate to the purpose of the processing, but not more than 30 days, except in cases expressly provided for by the law or in cases duly justified.

Thus, there are no restrictions per se in terms of monitoring and limiting the employees' use of computer resources, but it is mandatory before engaging in such activities to observe the provisions of both the GDPR and Law 190/2018.

8. SCOPE OF TELECOMMUNICATIONS REGIME

8.1 Scope of Telecommunications Rules and Approval Requirements

Government Emergency Ordinance No 111/2011 on electronic communications ("GEO 111/2011") transposes the main EU legal provisions in the field of electronic communications and covers all activities in the field of electronic communications networks and services.

According to GEO 111/2011, an electronic communications service is a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.

The provision of electronic communications networks and services is subject to (i) a general authorisation regime and, where applicable, (ii) licences for the use of limited resources for the provision of electronic communications net-

works and services (such as radio frequencies, numbering resources and other associated technical resources).

The procedure to become an electronic communications network and/or services provider under the general authorisation regime is free of charge and consists of a notification to the National Authority for Management and Regulation in Communications (ANCOM).

Instant Messaging

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code ("European Electronic Communications Code"), which came into force on 21 December 2018, extended the scope of electronic communication services. According to this European enactment, electronic communication services encompass the following types of services:

- internet access services;
- interpersonal communications services; and
- services consisting wholly or mainly in the conveyance of signals, such as transmission services used for the provision of machine-to-machine services and for broadcasting.

The concept of interpersonal communications services is new and refers to services normally provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s). This concept does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

There are two types of interpersonal communications services, namely:

- number-based interpersonal communications services, where the interpersonal communications service connects with publicly assigned numbering resources or enables communication with a number or numbers in national or international numbering plans; and
- number-independent interpersonal communications service, where the interpersonal communications service does not connect with publicly assigned numbering resources or does not enable communication with a number or numbers in national or international numbering plans.

The number-independent interpersonal communications services include instant messaging services such as WhatsApp and Facebook Messenger. According to the European Electronic Communication Code, the National Regulatory Authorities (NRAs) have powers with regard to instant messaging services consisting of, among others, submitting requests for information, settling dispute resolutions (including potential cross-border disputes), monitoring the market and protecting end-user rights with regard to non-discrimination, providing information in contracts, ensuring transparency and the quality of service.

The European Electronic Communication Code should have been transposed into the national legislation by 21 December 2020. However, at the date of publication this had not been transposed into Romanian law.

Voice over Internet Protocol

In Romania, Voice over Internet Protocol (VoIP) services using numbering resources are electronic communication services similar to fixed telephony services provided over public switched telephone networks (PSTNs). VoIP

services are subject to GEO 111/2011 in terms of numbering resources, number portability, interconnection, quality of service and access to emergency services.

RFIDs

In accordance with the telecoms framework, RFIDs are radio-frequency identification devices. The National Authority for Management and Regulation in Communications Decision No 311/2016 on radio frequencies and frequency bands, exempted from the licences regime, sets the technical specifications applicable to RFIDs.

9. AUDIO-VISUAL SERVICES AND VIDEO CHANNELS

9.1 Audio-Visual Service Requirements and Applicability

The main pieces of legislation regulating audio-visual media services in Romania are Law No 504/2002 on audio-visual content ("Audio-visual Law") and Decision No 220/2011 on the Code of regulation of audio-visual content ("Audio-visual Code").

Analogue programme services may only be provided by a broadcaster under Romanian jurisdiction on the basis of the analogue audio-visual licence and, as the case may be, of a broadcasting licence.

Digital terrestrial programming services through a broadcasting/television multiplex operator under Romanian jurisdiction may only be provided on the basis of a licence for the use of radio frequencies in a digital terrestrial system, for the benefit of digital audio-visual licence holders.

Procedure for Granting Audio-visual Licences

The procedure for granting audio-visual licences is provided in Decision 277/2013 of the National Audio-visual Council (CNA) on the procedure for granting, amending, extending the validity and assignment of the licence and the audio-visual authorisation decision, except for those for digital terrestrial broadcasting, as well as the conditions for the broadcasting of local programmes, retransmissions, or takeover programmes of other broadcasters.

For terrestrial frequencies, the licence is granted based on competition among providers. If the service is provided via electronic communication networks, the licence is granted by decision of the CNA.

Both analogue or digital audio-visual licences are granted for a period of nine years, for both radio and television. They can be renewed every nine years.

The holder of the broadcasting licence or the licence for the use of radio frequencies in the digital terrestrial system has an obligation to pay, annually in advance, a tariff for the use of the spectrum.

Video-on-demand services are governed by CNA Decision No 320/2012 regarding the provision of video-on-demand services. The decision does not apply to websites that provide user-generated audio-visual content for sharing, or sharing within a community of interest, such as YouTube.

The provision of on-demand audio-visual media services through electronic communications networks using digital terrestrial television systems is possible only on the basis of a digital terrestrial audio-visual licence granted by the CNA in accordance with the law.

Other than that, any person intending to provide on-demand audio-visual media services has an

obligation to notify the CNA of this intention at least seven days before the start of the activity.

The provisions of the Audio-visual Law and the Audio-visual Code apply accordingly to the audio-visual programmes broadcast on demand, considering their specificity to be viewed on request and at the time chosen by the user.

EU Directives Regulating Audio-visual Services

Romania is currently in the process of adopting legislation transposing the following EU directives:

- Directive (EU) 2018/1808 amending Directive 2010/13/EU on the co-ordination of certain provisions laid down by law, regulation or administrative action in member states concerning the provision of audiovisual media services ("Audiovisual Media Services Directive") in view of changing market realities – the Draft Law has been adopted by the chamber of deputies and is now pending voting in the senate;
- Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC – the Draft Law is under assessment in the chamber of deputies; and
- Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes and amending Council Directive 93/83/EEC – the Draft Law is under assessment in the chamber of deputies.

The directives regulate, among others, the regime of content-sharing platforms. Once transposed, Romania will have a regulatory regime for video-sharing platforms.

10. ENCRYPTION REQUIREMENTS

10.1 Legal Requirements and Exemptions

INFOSEC Directives

The main legislative acts related to encryption in Romania are in the field of protection of classified information. They include the so-called INFOSEC Directives, national acts issued by the Office of the National Register of State Secret Information (ORNISS).

Order 16/2014 for the approval of the Main Directive on INFOSEC, INFOSEC 2 ("INFOSEC Directive – INFOSEC 2") is the act which lays down guidelines for the security of information and communication systems ("SIC") in order to protect classified information stored, processed, or transmitted through it, with a view to ensuring confidentiality, integrity, availability, authenticity and non-repudiation.

The INFOSEC Directive – INFOSEC 2 applies to SIC which store, process or transmit classified information. It may also be applied to the protection of national classified information deemed as trade secrets, as well as of NATO or EU information which is not classified but which has administrative or dissemination limitation markings.

Cryptographic Products

For cryptographic products, an evaluation methodology was adopted in 2012 by order of ORNISS (Order 21/2012 on the approval of the Methodology for evaluation and certification of packages, products and protection profiles INFOSEC-INFOSEC 14). ORNISS is responsible for co-ordinating the certification processes of all INFOSEC-regulated products intended for

use at the national level, for which inclusion in the National Catalogue of INFOSEC protection packages, products and protection profiles is requested.

The evaluation and certification of cryptographic products are performed by two evaluating entities belonging to two of the following institutions: the Foreign Intelligence Service, the Romanian Intelligence Service, or the Ministry of National Defence.

Romanian legislation also requires entities acting in certain fields to use encryption. These include:

- investment funds and other such entities, which must ensure that relevant encryption technologies are used, where necessary, for certain types of data; these must be combined with appropriate security key management solutions, to limit the risk of unauthorised access to encryption keys; in particular, subjects must consider the latest technology and processes when choosing their security key management solution (Guide of 2021 of the Financial Supervisory Authority regarding outsourcing to cloud providers);
- holders of nuclear authorisation, which must implement, as a minimum physical protection measure, encryption of information when such information is transmitted (Norm of 2021 of physical protection in the nuclear field, issued by the National Commission for the Control of Nuclear Activities); and
- lawyers, who must choose secure online platform providers, and must ensure the protection of the information transmitted, so that the confidential data entered by the user on the site is protected by encryption and cannot be viewed by unauthorised persons (Decision 195/2021 for amending and supplementing the statute of the legal profession, adopted by the Decision of the Council of the National Union of Romanian Bars No 64/2011).

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

Currently, there are no specific enactments in connection with the COVID-19 pandemic that are relevant for the TMT sector.

However, in the National Recovery and Resilience Plan, Romania has allocated close to EUR2.8 billion for reforms and investments to support digital objectives. This is, among others, to help the transition to EU 2025 connectivity targets and to help stimulate private investment in the deployment of very high-capacity networks, as well as to implement a scheme to support the use of communication services through different types of instruments for beneficiaries, with a focus on white areas (areas where no telecoms infrastructure exists).

MPR Partners is an internationally recommended and award-winning law firm with a client-friendly, business-oriented and innovative approach. The firm's recognition comes from outstanding client feedback and reputed legal ranking and business publications at both international and local levels, as well as from its peers. With swift access to an extensive network of legal and tax professionals throughout the European Union and worldwide, an award-winning management team, competitive business terms and outstanding feedback from large corporations and international law firms, MPR Partners is a firm of choice for proficiently handled business law, tax and insolvency matters across the EU and beyond. Find out more on the firm's official websites: www.mprpartners.uk (London office) and www.mprpartners.com (Bucharest office).

AUTHORS

Alina Popescu is the founding partner of MPR Partners. She is an internationally commended lawyer with extensive expertise in legal management, M&A, competition law, technology and commercial and corporate projects, as well as in regulatory and international arbitration matters. Alina's diverse expertise, her ability to co-ordinate cross-border projects and her capacity to lead 365-degree, multi-angled assessments and strategies brings added value to the most intricate transactions and disputes. As a result, she has garnered outstanding feedback from major corporate clients and international law firms. She has been a qualified lawyer since 2004 and is a member of the International and Competition Sections of the New York State Bar Association, the International Bar Association, the International League for Competition Law and the Bucharest Bar.

Daniel Alexie provides valuable assistance to major corporate clients at MPR Partners with regard to various legal advisory matters, spanning IP, IT and telecoms, data privacy (assisting clients on adapting their corporate policy to comply with EU and Romanian privacy laws, including the upcoming General Data Protection Regulation) as well as advertising and consumer protection aspects. His expertise covers the M&A, corporate and commercial, competition and employment areas of practice. Daniel represents international and local clients in various sectors such as industry, services, entertainment and healthcare. He is a versatile and adaptable professional, showing team-player and good strategy-related skills, alongside the ability to multitask.

Flavia Stefura is part of MPR Partners' advisory department, being primarily involved in IP, data privacy, competition, consumer protection and M&A matters. She previously worked for reputed international law firms in the Romanian market, and deals with corporate and commercial, employment, regulatory as well as administrative matters. She advises high-profile clients that are active in various industry sectors, such as retail, FMCG, banking and finance. Flavia is a highly focused professional, delivering cross-departmental assistance in a timely manner.

Cristina Crețu is a senior technology and data privacy consultant at MPR Partners and has previously acted as a data privacy officer and regulatory manager with global telecoms companies, as well as a member of the legal team of a telecoms national regulator, having amassed vast hands-on expertise in data privacy, technology and telecommunications matters. She currently advises some of the world's largest corporations on data privacy, technology and telecoms matters, is a vice-chair of the American-Romanian Chamber of Commerce's Data Protection Task Force, and co-heads MPR Partners' task force on the Romanian National Council for Digital Transformation. She is a frequent contributor to reputed national and international publications.

MPR Partners

6A Barbu Delavrancea Street
Building C
Ground Floor
1st District
011355 Bucharest
Romania

Tel: +4021 310 17 17
Fax: +4021 310 17 18
Email: office@mprpartners.com
Web: www.mprpartners.com

Trends and Developments

Contributed by:
Alina Popescu and Cristina Crețu
MPR Partners see p.24

Introduction

The acceleration of the digitisation and digitalisation trends during the COVID-19 pandemic has led not only to a more stringent need for access to public and private services via digital means, but also to more pressing concerns regarding cybersecurity and potential threats from third-party state actors.

While the new technologies and the rapid development of the interoperability and interconnectivity of essential fields of activity are a driver for economic growth and social development, the ensuing challenges are not easy. These include fragmentation, interoperability, red tape around permits for network constructions, low digital skills, and exposure to cyber-risks.

Nevertheless, the reforms and investments provided in its National Recovery and Resilience Plan under the Digital Transformation component aim to ensure that Romania will have a coherent and integrated digital infrastructure which will help the transition to a more digitalised economy and society.

The importance of the topic is reflected in the budget allocated in Romania's National Recovery and Resilience Plan (endorsed by the European Commission in September 2021) to digital transformation-related investments, which represent a fifth of the total amount allocated under the plan.

In addition, Romania has continued to make headlines with its ever-flourishing technology sector, which has among other things seen a multibillion-dollar IPO, and Bucharest being designated as the venue of the EU Cybersecurity Competence Centre.

Technologies such as IoT, artificial intelligence, machine learning and 5G are expected to play an important role in Romania's economic growth, offering numerous opportunities for investments.

Digital Transformation in the Public Sector

The digitalisation of public administration plays a key role in Romania's National Recovery and Resilience Plan, with an emphasis on areas such as justice, employment and social protection, environment, civil service management and skills development, public procurement, cybersecurity, tax and customs. That adds up to a plan to build a secure government cloud infrastructure and to support the deployment of electronic IDs.

Romania also plans to invest in both:

- the digitalisation of health by developing an integrated e-Health system, which will help to connect over 25,000 healthcare providers and telemedicine systems; and
- the digitalisation of education, by improving digital pedagogical skills, educational content and equipment and resources.

The digital transformation is mainly focused on:

- setting up the government cloud;
- ensuring interoperability;
- improving connectivity;
- increasing the protection and cybersecurity of public and private entities; and
- increasing the digital competence of the public sector.

The process to ensure the digital transformation is to go hand in hand with the amendment of the Occupations Classification Code for the same to include the definition of new digital occupations.

Government Cloud

The Government Cloud is contemplated under two envisaged reforms.

- "Development of a unitary framework for defining the architecture of a government cloud"; and
- "Increasing digital competence for public service and digital education throughout the life of citizens" – this reform includes one investment which covers the deployment of the Government Cloud Infrastructure.

The National Recovery and Resilience Plan provides two legal enactments which are needed in order to develop a unitary framework for defining the architecture of a government cloud, namely:

- the Information Systems Interoperability Law, which will detail the uniform set of standards and rules that public entities are supposed to apply for the development of applications in a secure and sustainable environment; and
- the Government Cloud Act, which will set out the responsibilities and tasks regarding the design, implementation, development and management of the cloud infrastructure, technologies and services.

With regard to the Government Cloud Infrastructure, the National Recovery and Resilience Plan sets out four measures, namely:

- the construction of Tier IV and Tier III data centres by design;
- putting in place specific communication and information technology infrastructure;
- developing and expending support infrastructure such as electricity and physical security measures; and
- deploying scalable and high-availability information technology and communications (IT&C) infrastructure in each data centre.

5G networks

High-capacity networks and the necessary measures to ensure the transition to EU 2025 connectivity targets are both required in view of the digital transformation.

Stimulating private investment for the deployment of high-capacity networks, including through the acceleration of the national roll-out of 5G networks and through the provision of broadband coverage for white areas (where no telecoms infrastructure exists) has therefore become crucial.

In this respect, Romania is expected to take the necessary steps so that the auction for granting 5G licences may take place in the foreseeable future. This includes the transposition into national legislation of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code ("European Electronic Communications Code").

Broadband coverage and speeds

With a view to ensuring the provision of broadband coverage for white areas, the National Recovery and Resilience Plan envisages the implementation of a scheme to support the use of communication services through different types of instruments for beneficiaries, with a focus on white areas. This scheme is meant to help with the provision of coverage for very high-speed internet access, namely at least 100 Mbps delivered through FTTB/H and/or 5G networks to those areas where the market cannot

deliver these services on its own, ie, disadvantaged rural areas.

In order to address (i) the areas not covered with fixed networks, but which have a demand for services; and (ii) the fixed networks which do not provide for the necessary speeds to offer proper electronic communication services, investments are to be made in passive infrastructure and active network elements, backhaul and access segment, as well as in deploying new networks and upgrading the existing ones.

eHealth and telemedicine system

The pandemic increased the demand for telemedicine solutions. Although changes in the legal framework have been made to accommodate telemedicine, investments are needed in order to increase the access of rural and small urban areas, as well as of vulnerable groups, to specialised consultations via telemedicine.

The digitalisation of the National Health Insurance House and putting in place measures designed to ensure the cybersecurity of the Health Insurance IT Platform are two further important tasks for the Romanian authorities. In this respect, investments are planned to allow the integration of health institutions through digital infrastructure which will help to reduce fragmentation and increase the quality of health data.

eID and digital signature

The efforts towards the adoption of the eID are to continue, with the aim of facilitating digital interaction between citizens and public and private entities. Further to the investments set out in the National Recovery and Resilience Plan, Romania plans to deliver over eight million eIDs. The eID will enable the authentication process when using public administration online services and will offer the possibility of holding a qualified electronic signature issued by qualified certification service providers.

All reforms and investments mentioned above are envisaged to be carried out using non-reimbursable grants.

Cybersecurity

Bucharest is the host of the European Cybersecurity Industrial, Technology and Research Competence Centre (the "EU Cybersecurity Centre"), which should play an important role in connecting public stakeholders with the relevant researchers and private sector.

The aim of the EU Cybersecurity Centre is, among other things:

- to facilitate access by small and medium enterprises, start-ups or associations to knowledge by providing a helping hand in solving cybersecurity challenges, like the implementation of the security-by-design approach;
- to facilitate collaboration and the sharing of expertise among all relevant stakeholders; and
- to support the adoption and integration of state-of-the-art cybersecurity products, services and processes by public authorities at their request, by demand-side industries and by other users.

Having the EU Cybersecurity Centre in Bucharest will undoubtedly consolidate Romania's position as a significant actor in the field.

Contributed by: *Alina Popescu and Cristina Crețu,* ***MPR Partners***

MPR Partners is an internationally recommended and award-winning law firm with a client-friendly, business-oriented and innovative approach. The firm's recognition comes from outstanding client feedback and reputed legal ranking and business publications at both international and local levels, as well as from its peers. With swift access to an extensive network of legal and tax professionals throughout the European Union and worldwide, an award-winning management team, competitive business terms and outstanding feedback from large corporations and international law firms, MPR Partners is a firm of choice for proficiently handled business law, tax and insolvency matters across the EU and beyond. Find out more on the firm's official websites: www.mprpartners.uk (London office) and www.mprpartners.com (Bucharest office).

AUTHORS

Alina Popescu is the founding partner of MPR Partners. She is an internationally commended lawyer with extensive expertise in legal management, M&A, competition law, technology and commercial and corporate projects, as well as in regulatory and international arbitration matters. Alina's diverse expertise, her ability to co-ordinate cross-border projects and her capacity to lead 365-degree, multi-angled assessments and strategies brings added value to the most intricate transactions and disputes. As a result, she has garnered outstanding feedback from major corporate clients and international law firms. She has been a qualified lawyer since 2004 and is a member of the International and Competition Sections of the New York State Bar Association, the International Bar Association, the International League for Competition Law and the Bucharest Bar.

Cristina Crețu is a senior technology and data privacy consultant at MPR Partners and has previously acted as a data privacy officer and regulatory manager with global telecoms companies, as well as a member of the legal team of a telecoms national regulator, having amassed vast hands-on expertise in data privacy, technology and telecommunications matters. She currently advises some of the world's largest corporations on data privacy, technology and telecoms matters, is a vice-chair of the American-Romanian Chamber of Commerce's Data Protection Task Force, and co-heads MPR Partners' task force on the Romanian National Council for Digital Transformation. She is a frequent contributor to reputed national and international publications.

Contributed by: *Alina Popescu and Cristina Crețu,* ***MPR Partners***

MPR Partners

6A Barbu Delavrancea Street
Building C
Ground Floor
1st District
011355 Bucharest
Romania

Tel: +4021 310 17 17
Fax: +4021 310 17 18
Email: office@mprpartners.com
Web: www.mprpartners.com