MPR PARTNERS

GOING DIGITAL – ROMANIA's GOVERNMENT CLOUD SECONDARY LEGISLATION IN PLACE

1. Introductory remarks

It is no secret that Romania is the EU Member State with the least digitised services in the public administration. But that is about to change.

Having secured funding from the EU through the NextGenerationEU program, Romanian political leaders wish to create a secure and consolidated cloud infrastructure for the central administration institutions.

In lay terms, cloud computing refers to accessing computing resources (such as storage space, computer processors, software etc.) by users via the internet, instead of having them in the user's own space (on-premises/on-prem).

Cloud resources are commonly separated into infrastructure cloud services (infrastructure as a service – IaaS), platform cloud services (platform as a service – PaaS), and software cloud services (software as a service – SaaS).

Each Iaas, Paas and SaaS have different characteristics and roles. IaaS provides computing resources, through virtual computers, enabling a user to benefit from similar capabilities as a traditional data centre, but with the benefit of not having to go through the maintenance process. PaaS provides platforms for software creation, delivered online;

PaaS is used by software developers to create bespoke applications. SaaS typically delivers third-party managed applications to its users.

The Romanian government cloud will consist of all IaaS, PaaS and SaaS for the Romanian authorities, who will be the main users of the cloud. The Platform is purported to cover both interinstitutional workflows and the institutions' relationship with citizens.

This article will be an attempt to non-exhaustively describe the main characteristics and rules of governance of the Platform, as well as some of the problems raised by its implementation. The article is structured into four main parts. It starts by presenting the legal framework concerning the Platform. The second part presents the structure of the Platform; the third, rules of governance, with an accent on data regulation, and the last part is focused on the authors' remarks on the subject of the Platform's implementation.

2. Legal framework

In the summer of 2022, the Romanian Government issued the main framework for creating the future government cloud. The foundation of this framework consists of Government Emergency Ordinance no. 89 of June 28, 2022 regarding the establishment, management and development of infrastructures and cloud IT services used by public authorities and institutions ("**GEO 89/2022**").

GEO 89/2022 provides the general framework for the establishment, administration, and development, at national level, of a mix of private cloud and public clouds, amounting to a hybrid cloud which constitutes the Platform.

The general framework set out by GEO 89/2022 was to be accompanied by secondary legislation. After a long debate, the Romanian Government adopted Decision 112/2023 on the approval of the Governance Guide of the government cloud platform ("**GD 112/2023**") on February 8, 2023. Tertiary legislation (e.g., orders issued by the minister of research, innovation, and digitalization (hereafter "**minister of digitalisation**") approving specific contract templates, cloud service levels, management of the marketplace software applications etc.) is expected to follow still this year.

The law approving GEO 89/2022 has recently been voted on in the Romanian Parliament and will soon be published in the Official Gazette, ascertaining the legality of the GEO. The approving law does not substantially change the provisions of the GEO.

This article provides a quick overview of the intended structure of the Platform, as regulated by GEO 89/2022 and subsequent secondary legislation.

3. Platform structure

The Platform is intended as a hybrid cloud platform, which means that it has:

- a private cloud component (i.e., cloud services that service one client, and in this case are hosted on the infrastructure of the customer – the Romanian State); and
- a public cloud component (i.e., cloud services are hosted on shared infrastructure which is typically owned by a third party – e.g., cloud providers such as for example Microsoft, Google, Amazon, etc.).

Importantly, all technology used by authorities and institutions in the public sector will have to observe a "*cloud-first policy*", meaning that cloud will be considered before other technologies, whether for new IT and communications projects or technology upgrades for existing IT systems.

3.1. The private cloud component of the Platform

The private cloud component of the Platform ("**CPG**") will be set up by the Ministry of Research, Innovation and Digitalisation ("**Ministry of Digitalisation**") and the Authority for the Digitalisation of Romania ("**Digitalisation Authority**"), with the assistance of the Romanian Intelligence Service and the Special Telecommunications Service.

Central public administration authorities have the obligation to migrate electronic public services to the CPG. The migration of such authorities' own internal processes is optional.

All CPG components, (IaaS, PaaS, SaaS) will be state-owned. Once the CPG will be operational, the main priority will be migrating the central public authorities' applications in the CPG, a process which will be supervised by the Digitalisation Authority.

The types of services provided through the CPG will be established via order of the minister of digitalisation.

3.1.1. Specific authorisations needed for providing CPG components and applications

Importantly, the CPG is deemed part of the IT infrastructure of national interest.

IT infrastructure of national interest[1] is also the management tool representing the single-entry point for application programming interfaces (i.e., sets of rules and protocols allowing different software programs to communicate and share data or functionality)

[1] Defined by Law 163/2021 regarding the adoption of measures related to IT and communications infrastructures of national interest and the conditions for the implementation of 5G networks as the IT and communications infrastructure essential for maintaining the vital functions of society, the health, safety, security, social or economic well-being of individuals and whose disruption or destruction has a significant impact at the national level as a result of the inability to maintain the respective functions.

connecting the different institutions and authorities users of the Platform with one another ("**API Gateway**").

As a consequence, providers of IT solutions who will want to participate in tenders for building the CPG and/or the API Gateway will need to be authorised by the Prime Minister, based on the approval of the Supreme Council for Defence of the Country, as per the procedure set out in the Romanian legislation governing the authorisation of critical national infrastructure and 5G technologies.

This means that providers supplying CPG and API Gateway technologies, products, and services, will need to receive their authorisation no later than the date of the winning offer and the conclusion of the procurement contract. Due to rather long terms required for such authorisation to be obtained, it would be important for the authorisation process to be initiated as soon as reasonably practicable.

Open-source applications in the CPG and the API Gateway are not deemed infrastructure of public interest and therefore are not subject to the above-mentioned formalities. However, for any acquisition, provision or use of the open-source licensed software products, applications and services within the CPG and the API Gateway, prior approval from the Digitalisation Authority is needed instead. Such approval is to be granted based on the assessment of a technical body advising the Digitalisation Authority, to whom the documentation regarding the cloud services is to be submitted.

Thus, any provider who wishes to be a part of building or providing services within the CPG or API Gateway will need to be vetted by either the Supreme Council for Defence of the Country or by the Digitalisation Authority.

3.2. The public cloud component of the Platform

The public cloud component of the Platform consists of the privately-owned and operated software applications within a catalogue of cloud software applications available for Platform-hosted public institutions and authorities to use. This catalogue is called "marketplace".

Software applications in the marketplace can be either built for the Romanian State and owned by it or built and owned by private entities.

The complete list of applications and services offered within the Platform will be published in the marketplace and is to include:

- the name and description of the services;
- how to request and contract the services;
- service rates;

- service terms and conditions of use, as well as other information regarding their use.

The marketplace is managed by the Digitalisation Authority. Public institutions and authorities use the applications in the marketplace based on a contractual relationship established with the providers of the respective applications.

However, as will be seen below, the fact that a private provider has a software application registered in the marketplace does not guarantee that their application can be used by any of the public institutions and authorities registered in the Platform. The ability of public institutions and authorities to use applications of private providers may well depend on the type of data such authorities are processing and how they are processing the data.

4. Platform operation

GD 112/2023 sets out standards, rules, and obligations necessary for the operation of IT infrastructures and cloud services provided in connection to the Platform.

4.1. Main principles of operating the Platform

The Platform is regulated by a set of main principles, such as for example:

- the development and provision of cloud services centred on the needs of public authorities;
- the "cloud first" policy, according to which central authorities must use the Platform marketplace as their first option for use of applications and services; in addition, both central and local authorities have an obligation to prioritise acquiring cloud-native or cloud-ready applications and services in their investment plans;
- protecting data by ensuring secured access and adequate technical and cybersecurity measures; the measures imposed by the Romanian 5G legislation in this respect are equally applicable in the case of public clouds;
- one-time data upload – data subjects are only requested to share their personal data once; the data would then be accessed and further processed within the whole Platform by all the authorities that need it;
- compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**") in case of processing of personal data.

As is apparent from the above-mentioned principles, data (and especially personal data processing) is extremely important in the engineering of the Platform. More on the importance of data in the next section.

4.2. Data classification and data rules in the Platform

4.2.1. Data classification

Data stationed and transiting the Platform are classified as:

(i) personal data;

(ii) non-personal; and

(iii) special personal data[2].

According to GD 112/2023, special categories of personal data must be stored in data centres located in Romania, and, generally, personal data must be stationed on data centres in the EU, with the exclusion of overseas territories.

Moreover, special categories of personal data must only be hosted in the CPG or in other private clouds of the public authorities and institutions which are interconnected with the Platform.

General personal data and non-personal data can be hosted on any of the clouds present in the Platform.

Public institutions and authorities users of the Platform must classify the data they use prior to starting using the Platform, based on the entailed associated level of risk.

4.2.2. Protective measures for access to personal data

When travelling through the API Gateway, personal data must be encrypted. In other words, personal data must be encrypted when being exchanged between institutions or between institutions and cloud services providers.

Moreover, to ensure transparency of personal data processing, all accessing of personal data must be logged. Logs of access of data placed in the CPG are to be kept for a period of 36 months following their creation. They are also be presented to the relevant data subject upon request or through a notification in an application.

4.2.3. Cloud services providers as data processors

[2] These are the data provided at Article 9 of the GDPR, namely those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning a natural person's sex life or sexual orientation. Special categories of personal data are expressly provided by GDPR and no other data can be added to these categories, not even following a DPIA.

In most cases, cloud services providers will be processors of personal data on behalf of the public authorities using the Platform, and therefore will have to comply with the set of rules applying to processors.

Access to the data of the cloud services provider is generally not allowed, except for those situations regulated through the services contract. Access to personal data for corrective maintenance or technical assistance of the cloud IT applications or systems can only be done in the presence of a representative of the public authority having contracted the cloud service provider.

4.3. Conditions to ensure confidentiality, safety and interconnection

Cloud services providers must abide by certain rules to ensure data confidentiality, security, and interconnection, for example obligations to:

- provide clear details of any limitations, conditions or exceptions to the functionality and characteristics of the applications;
- describe the compatibility with other applications;
- state whether the applications are commercially available, under active development and supported until they are removed from the market, etc.

4.4. Main Platform actors and their responsibilities

The Platform generates relationships between several categories of actors:

- public authorities who are the users of the Platform (i.e., mainly the central administration public institutions and authorities);
- public authorities who are administrators of the Platform (i.e., mainly the Digitalisation Authority, the Ministry of Digitalisation, the Special Telecommunications Services, the Romanian Intelligence Services);
- private and public entities providing services in the Platform marketplace (i.e., the cloud service providers).

The Digitalisation Authority is the main actor in managing the Platform, with attributions to:

- conclude the services contracts with the user institutions and authorities in the CPG;
- conclude service level agreements[3];

[3] Agreements establishing the level of service expected from the public services providers, mainly the Special Communications Services and the Romanian Intelligence Services, as well as from the private services

- direct and manage the development of the Platform, also based on the analysis of public institutions and authorities' users' needs;
- monitor the adoption of cloud services and efficient use of resources by public institutions and authorities who are the users of the Platform;
- educate the personnel of the public institutions and authorities who are the users of the Platform in using cloud services;
- publish the minimal technical requirements for the applications which are allowed in the marketplace;
- validate and approve the applications which are allowed in the marketplace;
- ensure support and maintenance services for the marketplace;
- supervise and ensure the implementation of cybersecurity measures for the CPG and the API Gateway (cybersecurity attributions are shared with the Special Telecommunications Services and the Romanian Intelligence Services).

Public institutions and authorities using the Platform have a series of responsibilities to, among others:

- ensure the necessary resources for developing and maintaining own-commissioned cloud services;
- evaluate the risks and set the necessary security measures in accordance with the Platform standards;
- allocate the necessary resources and carry out compliance audits on security, data traceability and the quality of assigned cloud services;
- request, through the marketplace, the provision of cloud services made available by cloud services providers;
- manage its own information systems allocated on the Platform, including ensure licensing on operating systems (except when such licensing is ensured by the cloud services provider).

Cloud services providers are responsible among other things for:

- ensuring the availability and security of the services provided, within the limits of the agreed level of services;

providers, specifying the metrics by which service is measured, as well as remedies or penalties for non-observance of agreed metrics.

- providing, upon request, technical support for users;
- developing, installing, and managing the software components necessary for the proper functioning of the provided services;
- upon request, ensuring the integration of the provided services with other services;
- ensuring the protection of the data processed within the services, as well as the creation and storage of backup copies.

5. Comments and conclusions

5.1. Implications of data classification for cloud services providers

The main consequence of the data classification is that the special categories of personal data will only be processed by public authorities through the CPG, and not in the public cloud component of the Platform.

Additional rules concerning personal data, such as encryption, should be considered by both authorities and providers when tender books are written and when cloud services are delivered.

5.2. Points of concern from a data protection perspective

GD 112/2023 states that classification and management of data must be based on the risk level following a data protection impact assessment ("**DPIA**") performed in accordance with Article 35 of GDPR. However, as provided by Article 35 of GDPR, the scope of a DPIA is not to classify personal data, but to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. Moreover, a DPIA is not mandatory in all cases involving the processing of personal data, but it is limited by GDPR to those cases where the type of processing involves new technologies the use of which might result in a high risk for the rights and freedoms of natural persons.

Although cloud services might be deemed new technologies, not all data processing in the cloud might result in a high risk for the rights and freedoms of natural persons. Therefore, performing a DPIA should not be mandatory for all processing activities in the cloud. Given also that the entire process can prove to be quite burdensome for the public institutions and authorities, it should be analysed if a DPIA should be performed in the first place since a blanket obligation to perform it in all cases would not serve the purpose.

5.3. Points of concern from an IP perspective

The requirement to obtain intellectual property rights over all the software created for the Platform as a default will potentially cause conflicts in future tenders.

While licensing of intellectual property rights is also an option, Romanian authorities usually use standard drafting in tender books from this perspective. The wording is often that all intellectual property is to be transferred to the contracting authority.

For a sophisticated environment such as software development, where licensing and cross-licensing are usual, especially when open-source software is involved, potential bidders may raise (valid) issues with one-size-fits-all wording in tender books, and contestations to such conditions should not be surprising.

5.4. Next steps for the Romanian legislator to consider

Until the practical implementation of the Platform, more guidance should be enacted for both public authorities and cloud providers.

In discussing the tertiary legislation, more clarity should be provided on important issues, such as:

- the general terms and conditions for private-sector cloud providers accessing the Platform;
- the transfer of intellectual property rights or the mere licensing of it;
- streamlining public authorities' approach in requesting cloud services outside the CGP.

5.5. Conclusion

The Platform is definitely one of the most interesting and important developments of the last twenty years for public sector services. Since the pandemic, already the use of the existing patchwork of digital solutions of the local and central authorities has increased exponentially. For example, the website and, lately, app for paying taxes, ghiseul.ro, a successful model of public-private partnership in Romania[4], had 550,000 users in 2019[5], and, gradually, it reached about 1.6 million users by 2023[6].

However, the potential for growth is much greater. Romanian legislators have the important task of creating a legal regime that allows such growth to be reached sooner

[4] According to https://www.adr.gov.ro/autoritatea-pentru-digitalizarea-romaniei-a-organizat-evenimentul-de-prezentare-a-aplicatiei-mobile-ghiseul-ro-mai-simplu-mai-rapid-mai-sigur/, last accessed April 6, 2023.

[5] According to https://stirileprotv.ro/stiri/ilikeit/evolutia-platformei-ghiseul-ro-cati-romani-au-achitat-online-taxele-si-impozitele-in-ultimii-11-ani.html, last accessed April 6, 2023.

[6] According to https://economedia.ro/aplicatia-ghiseul-ro-a-fost-descarcata-de-80-000-de-ori-in-primele-cinci-zile-de-la-lansare.html#.Y_yR_R9Bw2w, last accessed April 6, 2023.

rather than later. Infusing rules and regulations with clarity, precision, and flexibility will definitely help achieve that goal.

Although a much awaited and necessary measure and even though important steps in the right direction, the legislation around Government Cloud Platform may need to be improved further. It can be expected that practical aspects of the implementation of the Platform will trigger the need for certain amendments and clarification in the legislation. Hopefully, some more clarity will for sure be provided by the adoption of the tertiary legislation.

***

Alina Popescu

Founding Partner (Bucharest & London)

alina.popescu@mprpartners.uk

Cristina Crețu

Partner (London)

cristina.cretu@mprpartners.uk

Flavia Ștefura

Managing Associate (Bucharest)

flavia.stefura@mprpartners.com