Chambers

GLOBAL PRACTICE GUIDES

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

TMT

Portugal

Law and Practice

Gonçalo Machado Borges, Nuno Peres Alves,
Vasco Stilwell d'Andrade and David Silva Ramalho
Morais Leitão, Galvão Teles, Soares da Silva & Associados

practiceguides.chambers.com

2021

PORTUGAL

Law and Practice

Contributed by:
Gonçalo Machado Borges, Nuno Peres Alves, Vasco Stilwell d'Andrade and David Silva Ramalho
Morais Leitão, Galvão Teles, Soares da Silva & Associados see p.11

Contents

Contributed by: *Gonçalo Machado Borges, Nuno Peres Alves, Vasco Stilwell d'Andrade and David Silva Ramalho, Morais Leitão, Galvão Teles, Soares da Silva & Associados*

1. Cloud Computing

1.1 Laws and Regulations

Recent years have seen a sizeable increase in migration by Portuguese corporate users of their IT infrastructure to cloud-based services. Cost reductions and efficiencies have been the main driver for this trend but other factors such as the self-service, flexible and scalable nature of cloud services have also contributed. Currently, according to IDC market figures, more than two-thirds of Portuguese organisations already resort to public or private cloud computing solutions and overall expenditure (of which software as a service, SaaS, is the main preferred service model) is projected to grow at an annual rate of 19.8% until 2023.

The Council of Ministers Resolution No 29/2020 encouraged the development of a legislative framework to facilitate research, simulation and testing activities, in a real environment, for innovative technologies, products, services, and models in Portugal (including, among others, artificial intelligence, blockchain, virtual reality, big data, 5G or Internet of Things), through the creation of Technological Free Zones.

Moreover, the Portuguese government recently introduced an Action Plan for Digital Transition through the Council of Ministers Resolution No 30/2020, which is considered an essential instrument for the country's development. This action plan foresees, in particular, a cloud strategy for the public administration, aiming to create a strategic framework for its integration in the cloud through the adoption of computing tools, and the digital transformation of businesses.

Laws and Regulations in Relation to the Cloud

In Portugal, there are no national laws or regulations specifically regulating cloud computing.

However, Law No 46/2018 of 13 August, which establishes the legal framework for security in cyberspace and transposes 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 (NIS Directive), defines "cloud computing services" as digital services that allow access to a scalable and adaptable set of shared computing resources (Article 3 (p)). It also qualifies the providers of such services as digital services providers (Article 11) to whom the cybersecurity regime applies.

Furthermore, in the context of entrusting processes or data to the cloud, certain limitations can nevertheless arise from general provisions (namely those governing the provision of services, consumer protection rules, IP law and data protection law). In practice, the contract terms between the cloud service provider and its client should stipulate, or circumvent, any relevant limitations.

General contract rules will apply to the formation and performance of cloud service contracts. These may vary from entirely standardised terms of service to more flexible and negotiated arrangements, with a content more tailored to the cloud service user's requirements.

Typical issues raised in the context of cloud computing service contracts include the following:

- compliance with data protection regulations imposed on the customers of a cloud services provider;
- liability in case of a security breach that involves a disclosure or a loss of confidential information and/or personal data;
- the question of the return or deletion of personal data and confidential information and the deadline to execute these actions after the conclusion of the services provided by the cloud service provider;
- the deadline for the cloud service provider to notify the customer of a personal data breach;
- technical and operative requirements to ensure the security of the information stored by the cloud service provider;
- SLA objectives and penalties, namely the time to solve technical problems which may lead to a lack of service access provided by the cloud service provider.

Industry-Specific Regulations/Guidelines

In Portugal, there is no industry-specific legal regulation in relation to the cloud. However, there are industry recommendations and guidelines, notably for the financial services industry.

The Portuguese Central Bank (*Banco de Portugal* or BdP), which is also the supervisory authority for the financial services sector, has stated its intention to ensure compliance with the European Banking Authority's (EBA) guidelines on outsourcing arrangements in its Carta Circular (guideline) No CC/2019/25. Although this refers explicitly to the 2017 Cloud Outsourcing Guidelines, these have been subsequently revised by the EBA in February 2019 and the current (and broader, covering also non-cloud outsourcing contracts) version is assumed to apply as of 30 September 2019.

Under the guidelines, specific requirements apply if the contracting of cloud-based services by a financial services provider constitutes a material outsourcing, involving the outsourcing to a cloud services provider of "critical or important" functions, such as those involving banking activities or payment functions.

Processing of Personal Data in the Context of the Cloud

The processing of personal data in the context of cloud computing is subject to the general rules on data protection established in the GDPR. Special attention should be given to the rules regarding data transfers to non-EEA countries, namely whether or not the transfers are made on the basis of an adequacy decision and whether appropriate safeguards for data protection are in place.

If a cloud services provider has a data centre in a non-EEA country, that factor should be taken into account. Also, attention and due care should be given to the appropriate technical and organisational measures against unauthorised access, as well as the availability and integrity of the personal data stored in the cloud (eg, encryption of the personal data).

It should be noted that cloud service providers are processors in light of the GDPR. Therefore, according to Article 28 of the GDPR, an agreement should be concluded to regulate the processing of personal data carried out by the processor, which should include, inter alia, the identification of the processors contracted by the cloud service provider (ie, subprocessors).

Additionally, it is worth mentioning that it is not prohibited to use cloud service providers located outside the EEA. However, according to the GDPR, any transfer of personal data to non-EEA countries shall take place only if:

- the European Commission has decided that the country in question ensures an adequate level of protection for personal data;
- the controller or processor has provided appropriate safeguards (eg, standard contractual binding clauses), and on condition that enforceable data subjects' rights and effective legal remedies for data subjects are available; or
- in the absence of an adequacy decision from the European Commission and of appropriate safeguards, and on an exceptional basis*:
  - (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
  - (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request and the transfer of personal data is occasional;
  - (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
  - (d) the transfer is necessary for important reasons of public interest;
  - (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
  - (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
  - (g) the transfer is made from a register which, according to EU or member state law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or member state law for consultation are fulfilled in the particular case.

* According to Article 29 Working Party – which was the independent EU Advisory Body on Data Protection and Privacy and which, with the entry into force of the GDPR on 25 May 2018, has been replaced by the European Data Protection Board – these derogations are exceptions from the rule that personal data may not be transferred to a non-EEA country unless the country provides for an adequate level of data protection or appropriate safeguards are put in place.

2. Blockchain

2.1 Legal Considerations

Blockchain (or distributed ledger) technology may be described as an encrypted database which keeps an irreversible and updated record of transaction information. The blockchain database compiles transactions in blocks, which are time-stamped, and distributed across a network of peer-to-peer participants (decentralised model). An integral copy of the database is stored in each of the network's computers, or nodes. To date, although many other potential applications hold enormous interest, blockchain has mainly been used in the context of cryptocurrencies and digital financial transactions.

With the recent publication of Law No 58/2020, of 31 August, implementing Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, *Banco de Portugal* has taken on the supervision of entities that manage virtual assets, or cryptocurrencies, in compliance with the legal and regulatory provisions applicable to the prevention of money laundering and financing of terrorism (exclusively).

In particular, BdP is responsible for registering entities that perform "exchange services between virtual assets and fiat currencies or between one or more virtual assets", "virtual asset transfer services" and/or "custody or custody services and administration of virtual assets or instruments that allow controlling, holding, storing or transferring these assets, including private cryptographic keys".

It should also be noted that, following the publication of Law No 58/2020, of 31 August, the BdP launched a public consultation on a draft notice (and the respective explanatory memorandum) aimed at regulating the information and documentation:

- of the application for registration by entities wishing to carry out activities with virtual assets;
- of the requests for changes in the facts subject to registration by entities carrying out activities with virtual assets.

The public consultation terminated in December 2020 and its results are expected to be published soon.

Risk and Liability

Risk and liability issues will depend on the specific blockchain solutions or applications in question and on the blockchain's private/permissioned or public/permissionless network structure. In any circumstance, and given the lack of specific legal rules or regulations, it is advisable for all entities involved to carefully assess potential risk and liability implications and to set up an appropriate contractual framework regulating these matters. This will involve allocating liability between blockchain developers and platform operators (eg, for smart contracts), notably for system errors and failures, and between the latter and downstream users (in this case, probably through more standardised contract terms). In addition to contractual regulation, insurance coverage may be advisable depending on the extent of each participant's liabilities.

Risk has received greater regulatory attention in the context of cryptocurrencies. In line with similar moves by many other European central banks and regulatory authorities for the financial sector, *Banco de Portugal* has issued several public statements with warnings on cryptocurrencies, notably a statement addressing Bitcoin (November 2013) and a subsequent one addressing the risks of using cryptocurrencies in general (October 2014).

The Portuguese capital markets authority (CMVM) has also published similar warnings to investors. In November 2017 it issued a warning concerning the potential risks of ICOs (initial coin offerings) for investors. More recently, in July 2018, CMVM published a notice addressed to entities involved in ICOs on the legal qualification of tokens. In this notice, it emphasised the need for the legal nature of tokens being offered in an ICO to be assessed, notably as to the possible qualification as securities. CMVM further stated that tokens may, depending on a case-by-case assessment, qualify as (atypical) securities under Portuguese law.

Furthermore, in December 2020, the BdP also published a paper on crypto-assets, identifying as the main risks underlying the use of crypto-assets:

- volatility risk – ie, the risk associated to the fluctuation of the market value;
- operational risk, related to the unsupervised trading platforms;
- regulatory risk, due to different approaches from regulators, supervisors and other authorities;
- anonymity – ie, associated to the risk of crypto-assists being used for criminal purposes;
- tax invasion risk; and
- risk arising from the absence or definitory information.

Intellectual Property

Blockchain technology created for an application may be protected by Portuguese copyright law and the Portuguese legislation applicable to trade secrets. Under Portuguese law, it is harder to protect an application involving blockchain technology by means of a patent due to the exclusion of source and object code from patentability, except if there is an invention (technical contribution) embodied in that source or object code used with blockchain technology.

Data Privacy

Depending on the use case of a specific blockchain application, both personal and non-personal data may be used by participants and registered in the ledger. Where personal data is involved, several issues regarding compliance of the blockchain with the framework data protection rules of the GDPR have been raised and are currently subject to debate. In Portugal, for instance, the Portuguese Data Protection Authority (CNPD) has singled out the processing of personal data using blockchain technologies as one of the three topics for in-depth review in its Action Plan for 2020.

A factor of potential conflict between the blockchain architecture and data protection rules results from the fact that in a blockchain there is no single, centrally responsible, data controller; rather, data may be stored and processed or updated by all participants in the blockchain, in a decentralised design (which is an essential feature of blockchain technology and sets it apart from more traditional models relying on the intervention of trusted third parties). This may make it more difficult for data owners to enforce their rights under the GDPR.

Another point of tension is the apparent incompatibility between the blockchain's immutable or irreversible design, which seeks to prevent or minimise changes to data (as a crucial means of enhancing security and trust in the database) and the rights to rectification and erasure (right to be forgotten) which the GDPR guarantees to data subjects. Given the potential similarities, in some cases, between a blockchain's storage and verification of transaction information and the functions traditionally performed by public registry systems (eg, real estate or commercial registry) it seems plausible that the right to erase personal data in this context might warrant a more restrictive interpretation.

Service Levels

Service levels regarding the use of a particular blockchain application or platform should be defined and regulated in the relevant contracts between developer, platform manager and end-user, as applicable.

Jurisdictional Issues

The fact that a blockchain is distributed to multiple nodes that may be physically located anywhere, and potentially spread out across several jurisdictions, is certain to raise choice of law and jurisdictional issues in the event of disputes. As for other cases of cross-border activities, participants should address the matter by drafting clear choice of law and jurisdiction clauses in their contracts in order to establish an internal governance structure and determine the applicable law and dispute resolution process for a particular transaction, in particular in the case of private or permissioned networks. Compatibility of these contractual provisions with mandatory rules of private international law may need to be assessed on a case-by-case basis.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

3.1 Challenges and Solutions

Big data, machine learning and artificial intelligence (AI) do not have a specific legal or regulatory framework in Portugal but are increasingly topics of debate and study, notably with a view to the framing and adoption of regulatory frameworks in future. A new and mostly innovation-friendly regulatory paradigm seems to be emerging. An example of this new paradigm is a recent Issues Paper from the Portuguese Competition Authority on Technological Innovation and Competition in the Financial Sector, which has proposed the creation of regulatory sandboxes to encourage the development of fintech start-ups and new business models for the financial sector, namely to foster the emergence of "robo-advisers" – ie, investment advisory applications powered by AI.

Additionally, it should be noted that when personal data is processed in this context the requirements of the RGPD must be fulfilled. Special attention should be given to the rules regarding retention periods. According to the GDPR, personal data can only be kept while it is necessary for the purposes for which personal data was collected, and the controller shall establish retention periods of personal data which comply with this rule.

It is also worth mentioning that personal data which has been anonymised is no longer considered to be personal data as defined in the GDPR. Therefore, the requirements under GDPR do not have to be observed if personal data are anonymised.

In March 2019, the Portuguese government constituted a task-force composed of representatives of multiple public entities and charged with preparing a recommendation on the legislative changes required to enable the introduction of new technologies related to autonomous driving (self-driving cars) in the automobile sector. The recommendation in question has not yet been made available.

Morais Leitão has partnered with legal services AI provider Luminance, an AI platform for lawyers, in the development of a starter-pack of 15 legal clauses in Portuguese. These are now available to the approximately 190 law firms and organisations worldwide that deploy this machine-learning technology.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions on a Project's Scope

Internet of Things (IoT) projects have been developing at an interesting rate in Portugal. Although there are no particular restrictions bearing on the scope of these projects, there are concerns about certain issues, such as safeguarding personal data that may be conveyed between connected devices and relevant to the provision of a given service.

Currently, larger customers of IoT solutions have been expressing concerns about potential lock-in in the context of long-term contracts with their connectivity providers as alternative IoT standards are being developed in parallel. On the other hand, electronic communications operators have been striving to develop integrated solutions that add significant value to customers for specific applications, moving beyond the mere provision of mobile connectivity.

A particular potential restriction that has also been weighing on the deployment of machine-to-machine (M2M) projects is the possibility that local authorities or municipalities may decide to subject the roll-out of micro-cells to licensing procedures,

permits and specific fees. However, the enactment of Article 57 of the European Electronic Communications Code (approved by Directive (EU) 2018/1972 of the European Parliament and of the Council) and its implementation into Portuguese law should suffice to lay major concerns in this field to rest.

The Portuguese regulatory authority for electronic communications and the postal sector (ANACOM) sent the draft project for the transposition of the European Electronic Communications Code to the government and to Parliament at the end of last year. However, this January 2021, the new law on electronic communications in Portugal has not yet been approved.

During 2019, ANACOM also kicked off a procedure to approve a specific regulation with the object of creating a specific numbering range within the National Numbering Plan for M2M services, including the regulation of number format and length and of conditions associated to their use, with particular reference to number portability and extraterritorial use. The procedure is still pending.

5. Challenges with IT Service Agreements

5.1 Legal Framework Features

IT service agreements in Portugal are typically based on models and drafts imported from US agreements, given that the USA has historically been at the forefront of IT development and business. Indeed, one need only think of Microsoft, Google, Oracle, Amazon and IBM to see that most of the largest IT service providers in the world have US origins. As a consequence of this, most IT services agreements in Portugal follow the same general structure and have similar clauses to those that can be found in most other jurisdictions.

By and large, the main challenge in the negotiation and performance of an IT service agreement in Portugal is the SLA (service level agreement) goals. In other words, defining what the service level objectives and criteria are, how to handle defects of different severity and what the consequences are for non-compliance (eg, payment of penalties, accumulation of credits, etc).

In addition to the commercial conditions, which are often a major source of discussion, the liability of the parties and possible caps to such liability are also topics that frequently lead negotiations astray. Naturally, the greater the risks of IT failure for the client, the greater the importance of the liability issue in IT agreements with IT providers. By way of example, the financial and utilities sectors give great relevance to the IT supplier's liability since they are regulated sectors that are obliged to provide constant service to the end customer. In Portugal, it is not possible for parties to previously exclude all liability, a rule that is often difficult for some IT providers to accept.

The entry into force of the GDPR in May 2018 has also brought personal data protection to the forefront of IT service agreements. Data privacy has ceased to be a residual issue regulated by a single clause in the IT services agreement. It is now standard in any IT agreement for data privacy to merit its own lengthy appendix.

Finally, the SaaS (software as a service), IaaS (infrastructure as a service) and PaaS (platform as a service) models that have become commonplace over the last decade have raised many new and interesting issues in Portugal and abroad. One of the hot topics that currently surfaces in every major cross-border IT services agreement is how the payments foreseen in the agreement should be taxed (eg, from VAT, double taxation and withholding tax perspectives). Regarding this subject, clarity is still often lacking.

6. Key Data Protection Principles

6.1 Core Rules for Individual/Company Data

Core Rules Regarding Data Protection

The core rules regarding data protection in Portugal are set out in Regulation (EU) 2016/679 (GDPR) and in Law No 58/2019 of 8 August, which ensures the implementation in Portugal of the GDPR.

Another important set of rules regarding data protection is Law No 7/2009 (Labour Code), which establishes, in Articles 16 to 22, norms on data processing in the workplace, namely, rules pertaining to the processing of an employee's biometric data, the demand for medical exams as a condition for employment and the use of remote surveillance methods.

Distinction between Companies/Individuals

The GDPR lays down rules relating to the processing of personal data. According to the GDPR, personal data means "any information relating to an identified or identifiable natural person ('data subject')". Therefore, while data pertaining to natural persons is protected under the GDPR and Portuguese Law No 58/2019 of 8 August, there is no general framework for the protection of legal persons' data.

However, Portuguese Law No 41/2004 of 18 August, which regulates the protection of personal data in the electronic communications sector, contains specific provisions for the sending of unsolicited communications for direct marketing purposes to natural and legal persons.

Additionally, it should be noted that professional data of natural persons is considered personal data for the purposes of the GDPR (eg, professional mobile phone number). Only professional data exclusively concerning the legal person is not personal data in light of the GDPR (eg, the general telephone number of the company).

General Processing of Data

Under the GDPR, personal data must be processed lawfully, fairly and in a transparent manner, with respect for the principles of purpose limitation and data minimisation, with accuracy, only for the period necessary for the processing's purpose and with respect for the required organisational measures to ensure the data's integrity and confidentiality. Additionally, data subjects enjoy the rights to information, access, rectification, erasure, restriction of processing, data portability, object and to not be subjected to automated individual decision-making.

7. Monitoring and Limiting of Employee Use of Computer Resources

7.1 Key Restrictions

The monitoring of private use by employees of company computer resources is governed primarily by Article 22 of the Labour Code which establishes that, while every employee has a right to the privacy of any personal email communications and non-professional information he or she may send, receive or access, employers are entitled to set out rules for the use of company resources and email accounts.

The CNPD has published guidelines on the monitoring and limitation of employee use, for private or personal purposes, of company computer resources in an employment context; monitoring of an employee's personal email or social network accounts is not permitted, even if they are accessed through a company computer.

Resolution 1638/2013 of the CNPD states that the monitoring means adopted must have the least impact possible on employee privacy rights and the related data processing must be limited to what is strictly indispensable. Generic monitoring methodologies based on parameters applying to all employees must be preferentially implemented by companies (eg, monitoring of the overall number, cost and duration of voice calls, number of messages sent, type of file attachments and time spent browsing the internet) and are considered generally sufficient to detect situations of abuse. As for traffic data, monitoring should be limited to the time and duration of communications, avoiding details such as numbers called, email addresses or visited websites.

Personal data processed in this context may be maintained for a maximum of six months, notwithstanding its possible use in disciplinary or judicial proceedings. In addition, employees must be informed in advance of the company's monitoring procedures and the corresponding data processing purposes and limitations.

Rules governing the personal use of company computer resources must be submitted to a privacy impact assessment and set out in an internal regulation. Companies must establish safety measures to ensure that any access for monitoring purposes is traceable, including through the use of digitally signed logs and time-stamps, in order to allow for internal and external audits.

8. Scope of Telecommunications Regime

8.1 Scope of Telecommunications Rules and Approval Requirements

The scope of local telecommunications rules, contained in Law No 5/2004, amended 13 times since its publication (amended and restated by Law No 51/2011 and last amended by Decree-Law No 92/2017, which implemented Directive 2014/61/EU) covers any fixed and mobile communications services as well as wireless and satellite services.

In accordance with the EU regulatory framework for electronic communications, Articles 3 (ff) and 2 (1) (b) of Law No 5/2004 defines an "electronic communications service" as 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, without prejudice to the exclusion referred to in point b) of paragraph 1 of Article 2"; this referral excludes any services which exercise editorial control over content – ie, the "mere" transmission of content is included in the concept as opposed to the actual production of content.

Any services satisfying this definition are covered by the Portuguese telecommunications rules regardless of the underlying technology (given the principle of technological neutrality). VoIP (voice-over internet protocol) services are covered in accordance with a summary regulatory framework adopted by ANACOM in 2006, including the creation of a specific numbering range (30) for nomadic use. According to this framework, VoIP services are regulated, in equivalent terms to the provision of fixed telephony services over the PSTN, with regard to numbering resources (geographic numbering is available on fixed access VoIP services), number portability, interconnection, quality of service and access to emergency services.

As for the requirements for bringing a product/service to the market, under the general authorisation regime that also applies in Portugal – in line with the EU regulatory framework – no licence or authorisation is required for the provision of electronic communications networks or services. This applies to any of the services mentioned above, whether these are publicly available or not. The offer of electronic communications services only requires prior notification to ANACOM – the regulatory authority for the telecommunications and postal sectors, which also performs supervisory, audit and sanctioning functions – after which the network/service provider may commence activities. ANACOM maintains a register of all undertakings that offer electronic communications services.

Despite the above, any activity requiring the use of radio spectrum frequencies or numbering resources depends on the award, by ANACOM, of the respective individual rights of use.

9. Audio-Visual Services and Video Channels

9.1 Audio-Visual Service Requirements and Applicability

The main requirements for providing an audio-visual service are contained in the statutes governing television and radio broadcasting, respectively Law No 27/2007 (Television Law), last amended by Law No 74/2020, and Law No 54/2010 (Radio Law), last amended by Law No 78/2015.

The above-mentioned Law No 74/2020 was published on 19 November 2020 – though it will only enter into force 90 days after that date – and transposed into the Portuguese legal framework Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018. These amendments have widened the Television Law's material scope to regulate more closely the offer to the public of video sharing platforms and rules on their content.

Under both the Television Law and the Radio Law, broadcasting may only be performed by corporate persons or co-operatives that pursue these activities as their main corporate object. With regard to television activity, a minimum share capital is set forth in the above-mentioned law, whose amount depends on the service and coverage offered.

Both television and radio broadcasting activities are subject to a licence provided they require the use of terrestrial broadcasting spectrum. Licences are awarded by the media regulator (ERC) pursuant to a public tender launched by government decision. In the case of television, the licensing requirement applies to the organisation of free unrestricted access (free-to-air) channels and to the selection and aggregation of conditional access or per subscription channels. If the broadcasting services do not involve the use of radio spectrum, they are only subject to an authorisation by ERC. Moreover, the licenses or authorisations related to these activities are, generally, issued for a period of 15 years, renewable for equal periods. They are given to a specific entity and non-transferable and have as a condition the provision of those services in the generality of the national territory, including the Autonomous Regions (Madeira and Azores).

Applications to ERC for television or radio broadcasting licences must be decided within 90 days from the date they are accepted as complete. Applications for an authorisation must be decided by ERC within 30 days, or 15 days in the case of radio broadcasting.

The fees for obtaining a licence/authorisation for broadcasting activities are set out in Annex IV to Decree-Law No 70/2009. The award or renewal of a national licence to television and radio operators who require the use of spectrum cost, respectively, EUR286,518 and EUR28,662; fees are lower for licences with a merely regional or local geographic scope. The award or renewal of authorisations to television and radio operators cost, respectively, EUR28,662 and EUR3,774.

These activities shall both comply with the competition rules, and their legal frameworks prevent them from being exercised or financed, directly or indirectly, by political parties or associations, trade union organisations, or public associations, except if it is exercised exclusively through the internet or refers to conditional access channels.

The above requirements do not apply to companies with online video channels or streaming service providers, such as Netflix or Amazon Prime, for instance, which remain essentially unregulated.

10. Encryption Requirements

10.1 Legal Requirements and Exemptions

There are several laws which specifically require companies to use encryption technology to safeguard data integrity or otherwise establish duties related to encryption.

Law No 5/2004, which establishes the general framework for electronic communications, allows the national regulatory authority for communications (ANACOM) to require that electronic communications service providers supply the competent national authorities with the means to decrypt or decipher data, whenever those measures are offered to consumers. Under the rights of use to the mobile spectrum frequencies issued to the three mobile

network operators in Portugal, all are required to supply the competent national authorities with the aforementioned means.

Another important set of rules related to electronic communications is contained in Law No 32/2008 and Ordinance No 469/2009, which govern the retention and transmission of traffic and location data for the investigation of serious crimes. Here electronic communications service providers are required to encrypt the information transmitted through an asymmetric cipher, when fulfilling a request for traffic and/or location data made by the judicial authorities.

Similarly, Organic Law No 4/2017 and Ordinance No 237-A/2018, which govern the access to telecommunications and internet data by the Portuguese Intelligence Services, require electronic communications service providers to encrypt the information transmitted through an asymmetric cipher, when answering a request for traffic and/or location data made by intelligence officials.

Another instance where companies are required to encrypt data is found in Law No 34/2013 and Ordinance No 273/2013, which govern private security activities. Here private security companies are required to encrypt any surveillance footage captured by security cameras that is transmitted and to change the encryption key every six months.

Finally, Law No 46/2018, which transposes Directive (EU) 2016/1148, and Commission Implementing Regulation (EU) 2018/151, which together provide a general framework for network and information security, require that digital service providers adopt technical measures aimed at network and information security risk management, which may include the use of encryption.

The use of encryption does not exempt an organisation from following any rules.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

In the context of the pandemic, the Portuguese government has enacted specific legislation enabling electronic communications operators to adopt exceptional traffic management measures in order to prevent or mitigate network congestion during lockdown periods.

In particular, Decree Law No 10-D/2020 of 23 March was aimed at responding to the sizeable increase in traffic volumes (both voice and, especially, data) on fixed and mobile networks – due to work-from-home policies and a more intensive use of entertainment and interactive services – by adopting exceptional and temporary measures for the electronic communications sector, such as identifying critical electronic communications services and defining categories of priority customers.

Under this legislation, services defined as critical are to be given priority for purposes of service continuity and include the following:

- voice and SMS on fixed and mobile networks;
- continuous access to emergency services, including information on caller location, and issuance of warnings to the public;
- data services, on fixed and mobile networks, required to ensure a minimum set of broadband internet services (these include email, search engines, online teaching tools, online news, online shopping, job search, online banking, financial and insurance services, online services provided by public authorities and messaging services);
- free-to-air television broadcasting and digital terrestrial television.

When providing these critical services, network and service providers must prioritise several categories of customers, notably public sector entities mainly involved in the provision of healthcare, security and logistical services.

Decree Law No 10-D/2020 also temporarily exempted electronic communications network and service providers from complying with several obligations, such as certain quality of service parameters, the standard deadlines for responding to consumer complaints, defined time periods within which to ensure specific mobile broadband coverage obligations, and an extension of remote portability request implementation deadlines to five business days.

This exceptional set of rules was repealed in August 2020. However, due to the second lockdown in Portugal, reinstated in January 2021, obligations such as identifying critical electronic communications services and defining categories of priority customers have been (re)imposed by Decree Law No 14-A/2021 of 12 January.

It is also worth mentioning the adoption of other exceptional and temporary measures in response to COVID-19, namely those provided for in Law No 7/2020 of 10 April. This statute approved a set of rules aimed at prohibiting the suspension of supply of electronic communication services during the initial state of emergency and the following month, in cases where consumers were in financial difficulty due to the pandemic. This prohibition is still in force, at least during the first part of 2021.

Contributed by: Gonçalo Machado Borges, Nuno Peres Alves, Vasco Stilwell d'Andrade and David Silva Ramalho, Morais Leitão, Galvão Teles, Soares da Silva & Associados

Morais Leitão, Galvão Teles, Soares da Silva & Associados is a leading full-service law firm in Portugal, with a solid background of decades of experience. Broadly recognised, Morais Leitão is a reference in several branches and sectors of the law on both a national and an international level. The firm's reputation amongst both peers and clients stems from the excellence of the legal services provided. The firm's work is characterised by its unique technical expertise, combined with a distinctive approach and cutting-edge solutions that often challenge some of the most conventional practices. With a team comprising over 250 lawyers at a client's disposal, Morais Leitão is headquartered in Lisbon and has additional offices in Porto and Funchal. Due to its network of associations and alliances with local firms and the creation of the Morais Leitão Legal Circle in 2010, the firm can also offer support through offices in Angola (ALC Advogados) and Mozambique (HRA Advogados).

Authors

Gonçalo Machado Borges is a partner who heads the telecoms and media practice group at Morais Leitão. He is also a member of the firm's European law and competition team and regularly advises electronic communications network operators and unified communications service providers in antitrust, transactional and regulatory matters and civil and misdemeanour litigation. Gonçalo is a member of the Portuguese Bar Association (admitted in 1998) and of the Associação Portuguesa para o Desenvolvimento das Comunicações (the Portuguese Association for the Development of Communications) and recently served as a board member of the Portuguese Competition Lawyers' Association.

Nuno Peres Alves is a partner who co-ordinates one of the administrative and public procurement teams. He also focuses his activity on regulated sectors, with an emphasis on the telecommunications sector, regularly advising one of the national operators, as well as foreign companies, in matters before the relevant Portuguese regulatory authority. In this field, Nuno often participates in seminars, conferences and lectures in postgraduate studies. He is a member of the Portuguese Bar Association (admitted in 1998).

Vasco Stilwell d'Andrade heads one of the firm's corporate teams and co-coordinates Team Genesis. He works mainly in the intellectual property field, namely in protection strategy and implementation, licensing, assignments, valuation and litigation, frequently assisting in litigation matters involving trade marks, patents and copyright. Vasco is an accredited Industrial Property Agent (Agente Oficial da Propriedade Industrial) and a registered Professional Representative before the Office for the Harmonisation of the Internal Market.

David Silva Ramalho is a member of the litigation and arbitration team with vast experience in the areas of criminal and misdemeanour litigation and compliance, especially in the economic and financial areas; arbitration; and personal data privacy and protection. He is a member of the Portuguese Bar Association (admitted in 2013), a fellow at the Tech and Law Centre in Milan, a researcher at the University of Lisbon's Centre for Criminal Law and Criminal Studies, and a member of the editorial boards of the "Digital Evidence and Electronic Signature Law Review" and the "Competition & Regulation Journal" ("Revista de Concorrência & Regulação").

Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.

Rua Castilho, 165
1070-050 Lisboa
Portugal

Tel: +351 21 381 74 00
Fax: +351 21 381 74 99
Email: mlgtslisboa@mlgts.pt
Web: www.mlgts.pt