

Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top ranked lawyers

TMT

Portugal

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

[chambers.com](https://www.chambers.com)

2019

Law and Practice

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

Contents

1. Cloud Computing	p.4	7. Monitoring & Limiting of Employee Use of Computer Resources	p.5
1.1 Laws and Regulations	p.4	7.1 Employees' Restrictions on Computer Use	p.5
1.2 Regulations in Specific Industries	p.4		
1.3 Processing of Personal Data	p.4	8. Scope of Telecommunications Regime	p.6
2. Blockchain	p.4	8.1 Technologies within Local Telecommunications Rules	p.6
2.1 Risk and Liability	p.4		
3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence	p.4	9. Audiovisual Services and Video channels	p.6
3.1 Big Data	p.4	9.1 Main Requirements	p.6
4. Legal Considerations for Internet of Things Projects	p.4	10. Encryption Requirements	p.7
4.1 Restrictions Affecting a Projects' Scope	p.4	10.1 Legal Requirements Governing the Use of Encryption	p.7
5. Challenges with IT Service Agreements	p.4	10.2 Exemptions	p.7
5.1 Specific Features	p.4		
6. Key Data Protection Principles	p.5		
6.1 Core Rules Regarding Data Protection	p.5		
6.2 Distinction Between Companies/Individuals	p.5		
6.3 General Processing of Data	p.5		
6.4 Processing of Personal Data	p.5		

Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL is a leading full-service firm that has a team consisting of more than 200 lawyers. Morais Leitão has its head office in Lisbon and offices in Porto and Funchal (Madeira Island). To support clients' international strategies, it has developed the Morais Leitão Legal Circle, a network of associations with local firms in Angola, Mozambique, Macau and Hong Kong that offers integrated multi-jurisdictional teams. The TMT team is divided into three practice groups:

telecoms and media, data protection, and the Legal Circle gaming practice. The key areas of practice in relation to the TMT sector are public law, European and competition law, litigation and corporate (with experience in the telecommunications, IT and media sectors). Since 2001 Morais Leitão has been the exclusive member firm in Portugal of Lex Mundi, the leading global network of independent law firms, through which it can provide clients with preferred access to more than 21,000 lawyers around the world.

Authors



Gonçalo Machado Borges is the managing associate of Morais Leitão. He is a member of the firm's European law and competition team, and co-ordinates the firm's telecoms and media practice group. Gonçalo, who is highly experienced in

telecommunications and media law, is a member of the Portuguese Bar Association (admitted in 1998), the Associação Portuguesa para o Desenvolvimento das Comunicações (the Portuguese Association for the Development of Communications) and, from 2017-19, a board member of the Portuguese Competition Lawyers' Association.



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').



Nuno Peres Alves is a partner who co-ordinates one of the firm's 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).

1. Cloud Computing

1.1 Laws and Regulations

In Portugal, there are no national laws or regulations specifically regulating cloud computing. 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 will stipulate, or circumvent, any relevant limitations.

1.2 Regulations in Specific Industries

In Portugal, there is no industry-specific regulation in relation to the cloud.

1.3 Processing of Personal Data

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 the transfers are made on the basis of an adequacy decision or not and whether appropriate safeguards for data protection are in place.

2. Blockchain

2.1 Risk and Liability

Legal issues surrounding the use of blockchain technology have not crystallised sufficiently in Portugal and we are not aware of any locally relevant inputs on the more or less universal questions that are being discussed worldwide (jurisdiction, validity/enforceability of smart contracts, transaction security, privacy versus immutability, etc). Certain soft law instruments have been published emphasising the potential associated to blockchain – such as the Portuguese Competition Authority's Issues Paper on Technological Innovation and Competition in the Financial Sector – but nothing of a regulatory nature. A more intensive awareness and use of blockchain technology involving Portuguese players will contribute to greater debate on possible solutions to legal challenges raised.

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

3.1 Big Data

Big data, machine learning and artificial intelligence are important topics in the Portuguese regulatory scene. While there is no specific regulatory framework for any of these technologies, a new and innovation-friendly regulatory paradigm seems to be emerging. An example of this new paradigm is the Portuguese Competition Authority's Issues

Paper 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' – investment advisory applications powered by AI.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions Affecting a Projects' 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 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.

5. Challenges with IT Service Agreements

5.1 Specific 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) 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 Regarding Data Protection

The core rules regarding data protection in Portugal are set out in Regulation (EU) 2016/679 (the GDPR). Given their overlapping scopes, the GDPR has rendered Law no 67/98 inapplicable in most respects, except, notably, for the criminal norms set out in Articles 43 to 49. A new Data Protection Law, aimed at executing the GDPR in Portuguese Law, is currently undergoing the legislative process; however, there is no current estimate as to when it will be approved or enter into force.

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, norms 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.

6.2 Distinction Between Companies/Individuals

While data pertaining to individual persons is protected under the GDPR, there is no general framework for the protection of corporate data.

6.3 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.

6.4 Processing of Personal Data

See 6.3 General Processing of Data.

7. Monitoring & Limiting of Employee Use of Computer Resources

7.1 Employees' Restrictions on Computer Use

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 e-mail 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 e-mail accounts.

The Portuguese Data Protection Authority (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 e-mail 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, e-mail 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 timestamps, in order to allow for internal and external audits.

8. Scope of Telecommunications Regime

8.1 Technologies within Local Telecommunications Rules

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 define 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 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 or 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 applies in Portugal also – 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 – 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. Audiovisual Services and Video channels

9.1 Main Requirements

The main requirements for providing an audiovisual service are contained in the statutes governing television and radio broadcasting, respectively Law no 27/2007 ('Television Law') and Law no 54/2010 ('Radio Law'), both last amended by Law no 78/2015.

Under both the Television and the Radio Laws, television and radio broadcasting may only be performed by corporate persons or co-operatives that pursue these activities as their main corporate object.

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.

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 (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.

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 Governing the Use of Encryption

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.

10.2 Exemptions

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

**Morais Leitão, Galvão Teles, Soares da
Silva & Associados**

Rua Castilho, 165
1070-050 Lisboa
Portugal

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

Tel: +351 213 817 400
Fax: +351 213 817 499
Email: mlgtslisboa@mlgts.pt
Web: www.mlgts.pt