

Chambers

GLOBAL PRACTICE GUIDES

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

Cybersecurity

Portugal

Gonçalo Machado Borges and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

practiceguides.chambers.com

2021

Law and Practice

Contributed by:

Gonçalo Machado Borges and Tiago Félix da Costa

Morais Leitão, Galvão Teles, Soares da Silva & Associados see p.11



Contents

1. Basic National Regime	p.3	5.3 Systems Covered	p.7
1.1 Laws	p.3	5.4 Security Requirements for Medical Devices	p.7
1.2 Regulators	p.3	5.5 Security Requirements for Industrial Control Systems (and SCADA)	p.7
1.3 Administration and Enforcement Process	p.3	5.6 Security Requirements for IoT	p.7
1.4 Multilateral and Subnational Issues	p.4	5.7 Reporting Triggers	p.7
1.5 Information Sharing Organisations	p.4	5.8 “Risk of Harm” Thresholds or Standards	p.8
1.6 System Characteristics	p.4		
1.7 Key Developments	p.4	6. Ability to Monitor Networks for Cybersecurity	p.8
1.8 Significant Pending Changes, Hot Topics and Issues	p.5	6.1 Cybersecurity Defensive Measures	p.8
2. Key Laws and Regulators at National and Subnational Levels	p.5	6.2 Intersection of Cybersecurity and Privacy or Data Protection	p.8
2.1 Key Laws	p.5		
2.2 Regulators	p.5	7. Cyberthreat Information Sharing Arrangements	p.8
2.3 Over-Arching Cybersecurity Agency	p.5	7.1 Required or Authorised Sharing of Cybersecurity Information	p.8
2.4 Data Protection Authorities or Privacy Regulators	p.5	7.2 Voluntary Information Sharing Opportunities	p.8
2.5 Financial or Other Sectoral Regulators	p.5		
2.6 Other Relevant Regulators and Agencies	p.5	8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation	p.9
3. Key Frameworks	p.5	8.1 Regulatory Enforcement or Litigation	p.9
3.1 De Jure or De Facto Standards	p.5	8.2 Significant Audits, Investigations or Penalties	p.9
3.2 Consensus or Commonly Applied Framework	p.5	8.3 Applicable Legal Standards	p.9
3.3 Legal Requirements	p.5	8.4 Significant Private Litigation	p.9
3.4 Key Multinational Relationships	p.6	8.5 Class Actions	p.9
4. Key Affirmative Security Requirements	p.6	9. Due Diligence	p.9
4.1 Personal Data	p.6	9.1 Processes and Issues	p.9
4.2 Material Business Data and Material Non-public Information	p.6	9.2 Public Disclosure	p.9
4.3 Critical Infrastructure, Networks, Systems	p.6		
4.4 Denial of Service Attacks	p.6	10. Other Cybersecurity Issues	p.9
4.5 IoT, Supply Chain, Other Data or Systems	p.6	10.1 Further Considerations Regarding Cybersecurity Regulation	p.9
5. Data Breach Reporting and Notification	p.7		
5.1 Definition of Data Security Incident or Breach	p.7		
5.2 Data Elements Covered	p.7		

1. Basic National Regime

1.1 Laws

The basic legal framework for cybersecurity in Portugal is that resulting from:

- 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);
- Regulation (EU) 2019/881 of the European 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, repealing Regulation (EU) 526/2013 (Cybersecurity Act), which is directly applicable in Portugal;
- Regulation 303/2019, approved by the national regulatory authority for electronic communications (ANACOM), on the security and integrity of electronic communications services and networks;
- Law No 53/2008 of 29 August, which approved the National Security Framework;
- Law No 41/2004 of 18 August, implementing Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector;
- Law No 32/2008 of 17 July (implementing Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006), on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

Law No 5/2004 of 10 February (Electronic Communications Law), as amended, also foresees obligations applicable to operators providing public communications networks or publicly available electronic communications services. In particular, it establishes an obligation to take appropriate technical and organisational measures to prevent, manage and reduce the risks posed to security of networks and services.

In addition to the above, and complementing the Criminal Code, Law No 109/2009 of 15 September (the Cybercrime Law), sets out cybercrime offences and regulates the surveillance of communications and apprehension of evidence in electronic format.

As for enforcement and penalties, infringement of the main obligations set out in Law No 46/2018, notably the obligation for public services, essential services providers and digital services

providers to implement adequate technical and organisational measures to address security risks, constitutes a very serious regulatory offence, punishable with fines of up to EUR25,000 or EUR50,000, depending on whether the infringer is a natural or a legal person, respectively. Failure to notify incidents to the competent regulatory authority is also punishable with fines of up to EUR3,000 or EUR9,000, for natural and legal persons, respectively.

1.2 Regulators

The supervisory authority responsible for monitoring the application of the cybersecurity rules and principles in Portugal is the *Centro Nacional de Cibersegurança*, also known as the CNCS, instituted by Decree Law No 3/2012 of 16 January, subsequently amended by Decree Law No 136/2017 of 6 November.

As defined by law, the CNCS' mission is to "contribute to the free, reliable and secure use of cyberspace in Portugal, through the continuous improvement of national cybersecurity and international co-operation, in co-ordination with all competent authorities, and the implementation of measures and instruments required for the anticipation, detection, reaction and recovery of situations that, in the imminence of occurrence of incidents or cyber-attacks, may compromise the operation of critical infrastructures and national interests" (Article 2(2) of Decree Law No 3/2012, as amended).

Furthermore, Law No 41/2004 also imposes an obligation to notify data breaches specifically involving personal data to the Portuguese Data Protection Authority (CNPd) and, specifically in the electronic communications sector, network and service providers must notify the regulator (ANACOM) of information security breaches or loss of integrity that causes a serious disturbance to the operation of networks and services and has a significant impact on the continuity of those operations.

Therefore, ANACOM and CNPD are also supervisory authorities in the context of cybersecurity.

1.3 Administration and Enforcement Process

The regulatory offence procedure is split into two phases:

- an administrative phase, where the supervisory authority investigates the relevant facts and ultimately decides whether or not to impose a penalty; and
- a judicial phase (the "appellate" stage), where the respondent may challenge the supervisory authority's decision in court.

The Portuguese Regulatory Offence Act (Decree Law No 433/82, as amended) establishes that no penalty may be imposed

without the defendant first having been heard regarding all the facts under investigation.

After hearing the defendant, if the supervisory authority decides to impose a penalty, this decision, as well as the amount of any fine imposed, may be challenged in court.

Defendants in a regulatory offence procedure are assured most of the due process rights established in criminal procedure laws, notably the presumption of innocence, the right to produce and present evidence and the right to appeal against unfavourable decisions. However, in these procedures, the privilege against self-incrimination may be mitigated, since controllers and processors are obliged to co-operate with the CNCS, according to Article 7, paragraph 2 of Law No 46/2018 of 13 August – for example, by supplying the authority with documents required and responses to information requests in the investigation stage of the procedure.

1.4 Multilateral and Subnational Issues

Being an EU member state, most relevant cybersecurity regulation in Portugal is either European legislation or local legislation based on European instruments.

The first specific cybersecurity law in Portugal is Law No 46/2018 of 13 August, which establishes the legal framework for security in cyberspace and implements Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 (NIS Directive), concerning measures for a high common level of security of network and information systems across the European Union.

In March 2018, the Portuguese Government issued Council of Ministers Resolution No 41/2018, which defines technical guidelines to be adopted by public services regarding measures for the security architecture of networks and information systems. The aim is to define a minimum baseline regarding adequate technical and organisational measures to be adopted by such entities, pursuant to being GDPR-compliant.

Additionally, the Cybersecurity Act is directly applicable in Portugal.

Finally, Portugal is a party to the Budapest Convention on Cybercrime of the Council of Europe (CETS 185), a binding international instrument that serves as a guideline for any country developing national legislation against cybercrime and as a framework for international co-operation between state parties. The CNCS also works in strong co-operation with NATO, the European Commission, ENISA, the Information Sharing and Analysis Centres (ISACs) and the Organization for Security and Co-operation in Europe (OSCE).

The instruments above are national in scope.

1.5 Information Sharing Organisations

The CNCS is at the centre of governmental intervention in cybersecurity and liaises with other agencies and organisations. The criminal investigation police authority (*Pol cia Judici ria*) also has a special unit dedicated to the investigation of cybercrime and technological criminality, the UNC3T (*Unidade Nacional de Combate ao Cibercrime e   Criminalidade Tecnol gica*). In the academic field, several universities – such as *Instituto Superior T cnico* (IST) – have developed in-depth capabilities in the analysis and study of cybersecurity issues and regularly promote information sharing and specialised training in this field.

There is no defined public-private partnership for cybersecurity in Portugal. However, the authors note that the National Cyberspace Security Strategy 2019-2023 refers to a principle of complementarity, whereby the security of cyberspace is a shared responsibility between public and private players. The 2019-2023 Strategy also highlights the need to consolidate and promote the national capacity for knowledge of cybersecurity threats in a collaborative manner between national authorities and public and private sector entities.

1.6 System Characteristics

The Portuguese legal system follows the EU model, since Portugal is a member of the European Union. Additionally, Regulations issued by the European Union – such as the Cybersecurity Act – are directly applicable in Portugal.

The legal regime for cybersecurity in force in Portugal is recent and, for that reason, it still at the early stages of its interpretation and enforcement.

1.7 Key Developments

In the last 12 months, there were no legal developments in the cybersecurity regime.

However, it should be noted that the National Cybersecurity Centre (CNCS) has been prolific in publishing best practice guidelines, particularly in the context of the pandemic. In particular, it has made available on its website (www.cncs.gov.pt/en/) a series of documents directed at both organisations and individuals describing the best practices to be followed in different scenarios, such as home study, work-from-home, travelling and public offices.

It has also published guidance on the usage of various digital tools – such as Google Classroom and Meet, Microsoft Teams, Moodle and Zoom – and made available advice on online

meetings and webinars, together with precautions relating to the use of passwords, etc.

1.8 Significant Pending Changes, Hot Topics and Issues

Cybersecurity requirements for 5G networks will probably continue to be the hottest topic over the next 12 months. The European Commission approved an EU toolbox of risk-mitigating measures in January 2020, addressing issues related inter alia to network standardisation and supply chain risks. In Portugal, the public tender procedure for the award of spectrum licences for 5G has been successively delayed and is now, finally, ongoing; therefore, implementation of the risk-mitigation measures set out in the EU toolbox will be one of the main challenges for local mobile operators in the near future.

As for the future, the authors note that in December 2020, the Commission adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). This proposal will now be subject to negotiations between the co-legislators, and once adopted, member states will have to transpose the NIS2 Directive within 18 months.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

Law No 46/2018 applies in general, as a cybersecurity framework, to information networks and systems, notably those operated by public authorities, critical infrastructure operators, essential services and digital services providers. The GDPR, and Law No 58/2019 of 8 August – which regulates and ensures the enforcement of the GDPR in Portugal – apply to personal data specifically. ANACOM Regulation 303/2019 applies specifically to the integrity and security of electronic communications networks and services.

2.2 Regulators

The CNCS is the central authority in Portugal tasked with monitoring compliance with legal cybersecurity requirements. See 1.2 Regulators, 2.4 Data Protection Authorities or Privacy Regulators and 2.5 Financial or Other Sectoral Regulators for reference to other relevant regulatory bodies in the field of cybersecurity.

2.3 Over-Archiving Cybersecurity Agency

The overarching cybersecurity agency in Portugal is the CNCS, described in 1.2 Regulators.

2.4 Data Protection Authorities or Privacy Regulators

The Portuguese data protection authority (*Comiss o Nacional de Prote o de Dados*, or CNPD) has an important role when a breach of security occurs that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (ie, personal data breach).

In these cases, the CNCS acts in co-ordination with the CNPD, according to Article 7, paragraph 8 of Law No 46/2018 of 13 August.

2.5 Financial or Other Sectoral Regulators

The Portuguese central bank and supervisory authority for the banking sector (*Banco de Portugal*) held a public consultation during 2019 (consultation 2/2019) regarding draft guidelines on the reporting of cybersecurity incidents by financial institutions, which led to instruction 21/2019 that regulates the reporting of cybersecurity incidents in entities supervised by Banco de Portugal and in significant credit institutions supervised by the European Central Bank (ECB) having a registered office in Portugal.

In addition, cybersecurity incidents affecting credit institutions qualified as significant under Regulation (EU) 468/2018 of the European Central Bank of 16 April 2014, and having a registered office in Portugal must be reported directly to the ECB.

2.6 Other Relevant Regulators and Agencies

The key relevant regulators are those mentioned previously in this section. ANACOM, the regulatory authority for the electronic communications sector, is also a key regulator, notably regarding data breaches and network integrity and security requirements.

3. Key Frameworks

3.1 De Jure or De Facto Standards

Several standards provide guidance and are commonly relied upon, such as ISO/IEC 27032, ISO 22301, ISO/IEC 22000, ISO/IEC 27000, ISO/IEC 27001 and ISO 9000.

3.2 Consensus or Commonly Applied Framework

This issue has not arisen in this jurisdiction.

3.3 Legal Requirements

Written Information Security Plans or Programmes

As for written information security plans, there are standards applying to the specific items above which are defined in the CNCS's National Reference Framework for Cybersecurity under

a taxonomy of security measures defined in accordance with the following categories:

- identify;
- protect;
- detect;
- respond;
- recover.

This framework document seeks to provide organisations with a cybersecurity guide and set out minimum security information requirements.

Incident Response Plans

In regard to incident response plans, the CNCS provides a service – CERT.PT – that co-ordinates the response to incidents involving state entities, operators of critical infrastructure, operators of essential services, digital service providers and the national cyberspace in general.

Furthermore, other entities have action plans in force to respond promptly to eventual cyber-attacks. This is the case of *Banco de Portugal*, that published Regulation 21/2019 providing for the reporting of severe cybersecurity incidents affecting entities under its supervision and significant credit institutions based in Portugal that are supervised by the ECB.

ANACOM also establishes that electronic communications providers should prepare and maintain a security plan, duly documented and signed by the head of security, which must contain the security policy and a description of all measures taken with regard to the security of their networks and services (Regulation 303/2019 of 1 April, on the security and integrity of electronic communications networks and services).

In general, companies from all sectors are tending to follow stricter cybersecurity plans (even when not legally mandatory), especially considering the exponential growth in the number of such incidents over the last year.

3.4 Key Multinational Relationships

CNCS liaises on a regular basis with ENISA, ISACs (Information Sharing and Analysis Centres) and with the OSCE. The CNCS also works in close co-operation with NATO and the European Commission.

4. Key Affirmative Security Requirements

4.1 Personal Data

Security requirements are addressed in Article 32 of the GDPR (see also Recitals 74, 77 and 83) in relation to the security of processing personal data and include measures such as pseudonymisation and encryption of personal data, regular testing and assessment of technical and organisational measures as well as adherence to approved codes of conduct or certification mechanisms.

4.2 Material Business Data and Material Non-public Information

Currently, the authors identify no relevant affirmative security requirements in this jurisdiction regarding material business data or non-public information.

4.3 Critical Infrastructure, Networks, Systems

Critical infrastructure is covered by Decree Law No 62/2011 which, inter alia, sets out the need for each infrastructure identified as critical to have an own security plan including security measures regarding its information systems; see Article 10 (3) (e). There is also a 2017 best practices guide published by the National Platform for the Reduction of Catastrophe Risk, which explicitly refers the need to “implement measures for the protection of critical information systems, mitigating the risk of eventual cyberattack occurrences” (page 29).

Additionally, Law No 46/2018 also applies specifically to essential services providers, including suppliers in the following sectors: (i) energy, (ii) transportation, (iii) financial services, (iv) health, (v) water supply, and (vi) digital infrastructure, establishing a mandatory notification to CNCS in case of incidents having a relevant impact on network and information systems’ security.

4.4 Denial of Service Attacks

Currently, the authors identify no relevant affirmative security requirements in this jurisdiction regarding denial of service attacks or similar attacks.

4.5 IoT, Supply Chain, Other Data or Systems

ANACOM Regulation 303/2019 contains specific rules and obligations applying, specifically, to undertakings that offer public communications networks. These obligations extend to asset classification and inventory, to having and updating a security plan as well as reporting obligations (including an annual security report). Any breaches or loss of integrity incidents with a significant impact on the networks’ functioning must be reported to ANACOM. Several circumstances, such as number of subscribers affected or geographic scope of the incident, are laid out in the Regulation as relevant criteria

towards assessing whether an incident may cause serious harm to the operation and continuity of networks and services.

Furthermore, Law No 46/2018 defines “cloud computing services” as digital services that allow access to a scalable and adaptable set of shared computing resources (Article 3 (p)), and it qualifies the providers of such services as digital services providers (Article 11) to whom the cybersecurity regime applies.

As for the internet of things (IoT), the National Cyberspace Security Strategy 2019-2023 notes that the increase in internet-connected devices may contribute to a rise in the number or frequency of cyber-attacks. However, it does not indicate any particular measures or security requirements to be implemented in the short term.

5. Data Breach Reporting and Notification

5.1 Definition of Data Security Incident or Breach

Article 3 (c) of Portuguese Law No 46/2018 of 13 August defines an incident as an event having an actual adverse effect on the security of network and information systems.

5.2 Data Elements Covered

Networks and information systems must ensure the adequate protection of both stored data and data in transit.

5.3 Systems Covered

Law No 46/2018 covers cybersecurity requirements for information systems and networks in general, defined in accordance with the NIS Directive. These include electronic communications networks, devices or groups of interconnected devices that, pursuant to a program, carry out the automatic processing of digital data; and the digital data stored, processed, retrieved or transmitted by said networks or devices, for the purposes of their operation, use, protection and maintenance.

5.4 Security Requirements for Medical Devices

Operators of critical infrastructure (which include public or private entities who operate health-related components or systems) must notify the CNCS of any incidents with a relevant impact on network and information systems security (see Articles 3 and 15 (1) of Law No 46/2018 of 13 August).

5.5 Security Requirements for Industrial Control Systems (and SCADA)

This issue has not arisen in this jurisdiction.

5.6 Security Requirements for IoT

The eventual need for specific security measures regarding IoT devices has been identified by the CNCS although no guidelines or list of requirements have been published. Possible measures might include inhibiting wireless connections, ensuring access credentials are updated regularly, encrypting communications or mandating firmware updates.

5.7 Reporting Triggers

Government Authorities

Under the GDPR provisions fully applicable in Portugal, personal data breaches must be notified by the controller to the CNPD without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Notification to the CNPD is made online on an appropriate form made available by the authority in its public website (www.cnpd.pt/).

Law No 46/2018 of 13 August requires various service providers to notify the CNCS – the national competent authority in Portugal for both digital service providers and operators of essential services – in the event of cybersecurity incidents.

Under the implementation provisions, public administration and critical infrastructure operators shall notify the CNCS of incidents with a relevant impact in network security and information systems, within the period provided for in specific legislation. This notification must include information that allows the CNCS to determine the cross-border impact of the incidents.

Whenever the circumstances allow, the CNCS provides the notifier with the relevant information regarding the follow-up of the notification, namely information that may contribute to the efficient handling of the incident. After consulting with the notifier, the CNCS may disclose specific incidents, with respect to public interest, safeguarding the safety and the interests of critical infrastructure operators.

Operators of essential services notify the CNCS of incidents with a relevant impact on the continuity of essential services provided by them, within the period provided for in specific legislation. This notification must also include information that allows the CNCS to determine the cross-border impact of the incidents.

Providers of digital services must notify the CNCS of incidents with a substantial impact on the provision of digital services, within the period provided for in specific legislation. This

notification must include information that allows the CNCS to determine the significance of the cross-border impact. The obligation to notify an incident is only applicable if the digital service provider has access to the necessary information to assess the transborder impact of an incident. If these incidents concern more than one member state, the CNCS must inform the single contact point of the other member states involved.

Individuals

Pursuant to Article 44, paragraph 1 of the GDPR, when the personal data breach is likely to result in a high risk to the rights and freedoms of the affected data subjects, the controller shall communicate the personal data breach to the data subjects without undue delay.

5.8 “Risk of Harm” Thresholds or Standards

The relevance of any incident, whether it affects public services, operators of essential services, essential service providers or digital service providers, must be assessed in light of several criteria, including the number of affected users; the incident’s duration and its geographical distribution.

In the case of digital services (ie, online marketplaces, online search engines and cloud computing services), the seriousness of the disturbance to the service’s performance as well as the extent of its impact on social and economic activities must also be considered.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

Article 18 of the Portuguese Law No 109/2009 of 15 September (the Cybercrime Law) allows for the real-time interception of content and traffic data for the investigation of cybercrimes and crimes where wiretaps would be allowed under the Criminal Procedure Code. The real-time collection of data must be authorised by an investigating judge and must be indispensable for the investigation of the crimes at hand.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Cybersecurity and data protection, while being distinct areas with distinct concerns, often overlap. Notably, the legal frameworks for both cybersecurity and data protection require companies to implement adequate security measures to ensure the confidentiality, integrity and access to data, and also require companies to notify the competent authority in the case of security incidents. Furthermore, cybersecurity risks and measures will often be relevant when conducting a

Data Protection Impact Assessment, pursuant to Article 35, paragraph 7, subparagraphs c) and d) of the GDPR.

However, there may be cases where cybersecurity obligations may be at odds with individuals’ rights and freedoms, granted under data protection legislation, such as when network monitoring involves the processing of personal data. In such cases, cybersecurity concerns may be construed as a “legitimate interest”, pursuant to Article 6, paragraph 1, subparagraph f) of the GDPR, thus allowing for the lawful processing of personal data. Furthermore, cybersecurity measures may themselves warrant the performance a Data Protection Impact Assessment if the measures in question are likely to result in a high risk to the rights and freedoms of natural persons, pursuant to Article 35, paragraph 1 of the GDPR.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

Companies subject to Law 46/2018 are required to notify the National Cybersecurity Centre (CNCS) of any cybersecurity incidents with a substantial impact on their activities. The information shared depends on the kind of entity affected by the incident – critical infrastructure operator, essential services provider or digital services provider – but always includes, at least, the number of affected users, the duration and the geographical scope of the incident.

Moreover, under Article 33 of the GDPR, data controllers must notify the National Personal Data Commission (CNPd) of any personal data breach within 72 hours of its discovery. Notifications must include, at least: the nature of the personal data breach; the name and contact information of the Data Protection Officer or of another contact point; the likely consequences of the personal data breach; and a description of the measures taken or proposed to address the personal data breach.

In the telecoms sector, under Regulation 303/2019, providers are required to notify ANACOM of information security breaches. Furthermore, companies must draft a cybersecurity policy and keep it updated. A company’s cybersecurity policy must be sent to ANACOM within 20 days of the beginning of its activities. Providers are also required to draft an annual security report and send it to the regulator.

7.2 Voluntary Information Sharing Opportunities

Notwithstanding the above-mentioned obligation to notify incidents, any entities may voluntarily notify the CNCS of

incidents with a significant impact on the continuity of services provided by them, pursuant to Article 20 of Law No 46/2018 of 13 August.

The voluntary notification cannot give rise to the imposition of obligations to the notifying entity to which said entity would not have been subjected to had it not made that notification.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

Based on public information available, 2020 has seen a significant increase in the number and diversity of cybersecurity and data breach incidents in Portugal. EDP – the leading energy company in Portugal – suffered a cyber-attack in the second quarter of the year, in the course of which 10 TB of private information were allegedly hacked, with a ransom in bitcoin being demanded as a precondition to decryption of the data. More recently, a listed company was the object of a data leak and attempted ransomware attack.

In general, investigation of cybercrime involving ransomware, phishing, CEO fraud, money laundering (from drug trafficking, etc) via Bitcoin, as well as cyberharassment and cyberbullying is becoming more common and widespread.

8.2 Significant Audits, Investigations or Penalties

There are regulatory offences laid down in Law No 46/2018 of 13 August. These offences are divided between “serious offences” and “very serious offences”.

Very serious offences – which include non-compliance with the obligation to implement security requirements and non-compliance with the instructions of cybersecurity issued by the CNCS – are punished with (i) a fine of between EUR5,000 and EUR25,000, in case of an offence by a natural person, and (ii) a fine of between EUR10,000 and EUR50,000, in case of an offence by a collective entity.

Serious offences include non-compliance with the obligation to notify the CNCS of any incidents occurred, non-compliance with the obligation to notify the CNCS of activities carried out in the digital infrastructure sector, and the non-compliance with the obligation to notify the CNCS of the identification as a digital service provider. These offences are punished with (i) a fine of between EUR1,000 and EUR3,000, in case the offence is committed by a natural person, and (ii) a fine of between EUR3,000 and EUR9,000, in case the offence is committed by a collective entity.

Regarding private litigation, the general principles of civil law apply to data security incidents or breaches.

8.3 Applicable Legal Standards

The applicable legal standards refer, predominantly, to conduct that may qualify as being criminal in nature (under the Cybercrime Law) or to constitute a regulatory offence, notably punishable with fines, under Law 46/2018 of 13 August. In addition, to the extent responses to security incidents and breach situations involve access to or processing of personal data, data protection rules are also relevant, both under the GDPR and according to Law 58/2019 of 8 August, which adopted measures seeking to ensure the GDPR’s enforcement in Portugal.

For further information, please see **1.1 Laws** and **2.1 Key Laws**.

8.4 Significant Private Litigation

Private parties may have a right of action resulting from cybersecurity violations, which will normally arise from breach of contract, although claims based on tort grounds may also arise. However, to the extent of the authors’ knowledge, this issue has not arisen in this jurisdiction.

8.5 Class Actions

Portuguese Civil Procedure Law allows for class action lawsuits for the protection of consumer interests. However, to the extent of the authors’ knowledge, this issue has not arisen in this jurisdiction.

9. Due Diligence

9.1 Processes and Issues

This issue has not arisen in this jurisdiction.

9.2 Public Disclosure

The authors are not aware of any laws under this heading.

10. Other Cybersecurity Issues

10.1 Further Considerations Regarding Cybersecurity Regulation

Two recent trends stand out, which may encourage the adoption of additional, specific, cybersecurity regulation in Portugal in the near future.

Firstly, 2020 saw a significant increase in the number of cybercrime offences reported to the Cybercrime Desk of the public prosecution services. Following a steady increase since 2016, the number of complaints brought during 2020 increased exponentially to the point of doubling in number by the end of

the year. This increase was especially noticeable during March to May 2020, coinciding with the initial lockdown period determined by the Portuguese government in the context of the COVID-19 pandemic. The most representative types of offence include phishing practices, ransomware, CEO fraud, online fraud, cryptocurrency fraud, stalking and sextortion offences.

On the other hand, and specifically in the context of payment apps, there has also been a visible increase in multiple types of fraud involving the MBWay payment app. This is a mobile app specific to the Portuguese banking system which enables several payment services to be rendered from deposit accounts in most Portuguese banks. The MBWay app allows for payment of purchases or transfers between different accounts by associating a user's debit card to his or her mobile number; payments are authenticated by means of a PIN code.

The specific means by which fraud is perpetrated vary, but a common method is for fraudsters to identify potential targets among sellers on online platforms or marketplaces (notably if they provide a mobile contact number) who they then contact, purporting to be interested in purchasing the items advertised for sale. Victims are then deceived into either activating the MBWay service at a nearby ATM with a predefined PIN and associating it to the fraudsters' own mobile number or into accepting "send cash" messages which are actually requests for cash transfers sent by the fraudsters. Frauds involving this mobile payment system rely on securing access to the victims' bank account credentials through the app, thereby enabling fraudulent payments or transfers.

PORTUGAL LAW AND PRACTICE

Contributed by: Gonalo Machado Borges and Tiago F lix da Costa, Morais Leit o, Galv o Teles, Soares da Silva & Associados

Morais Leit o, Galv o 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 Leit o is a reference in several branches and sectors of the law on a national and 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 Leit o 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 Leit o Legal Circle in 2010, the firm can also offer support through offices in Angola (ALC Advogados) and Mozambique (HRA Advogados).

Authors



Gonalo Machado Borges is a partner who heads the telecoms and media practice group at Morais Leit o. 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. Gonalo is a member of the Portuguese Bar Association (admitted in 1998) and of the Associa o Portuguesa para o Desenvolvimento das Comunica es (the Portuguese Association for the Development of Communications) and recently served as a board member of the Portuguese Competition Lawyers' Association.



Tiago F lix da Costa is a partner and head of one of the litigation and arbitration teams – the criminal litigation, administrative sanctions/misdemeanour and compliance team – and co-ordinator of the data protection team. He joined the firm in 2007 and became a partner in 2015.

Having been a practitioner of law since 2004, Tiago has wide experience in the areas of criminal and misdemeanour litigation and civil, corporate and commercial litigation. Recently, Tiago has acted increasingly in the personal data protection sector, providing legal assistance on criminal and misdemeanour processes in this area and assisting several companies on the creation of policies and programmes of compliance in the personal data protection sector. Tiago is a member of the Portuguese Bar Association (admitted in 2004), regularly teaches postgraduates in different law faculties and has contributed to several publications relating to data protection law. Tiago holds certification from the Advanced Training Course on Data Protection Compliance in the EU (European Institute of Public Administration – EIPA, 2017).

Morais Leit o, Galv o Teles, Soares da Silva & Associados

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

M
L **MORAIS LEIT O**
GALV O TELES, SOARES DA SILVA
& ASSOCIADOS